

NN10037-111

Succession Multimedia Communications Portfolio

MCP Accounting Module

Basics

Standard MCP 1.1 FP1 (02.02) April 2003



Overview

ATTENTION

The accounting software is subject to updates for each maintenance release.

How this chapter is organized

This chapter is organized as follows:

- “Strategy” on page 3
 - “Local Accounting Manager (LAM)” on page 4
 - “Central Accounting Manager (CAM)” on page 5
 - “Hardware” on page 6
 - “Software” on page 6
 - “Tools and utilities” on page 7
 - “Understanding accounting attributes and events” on page 7

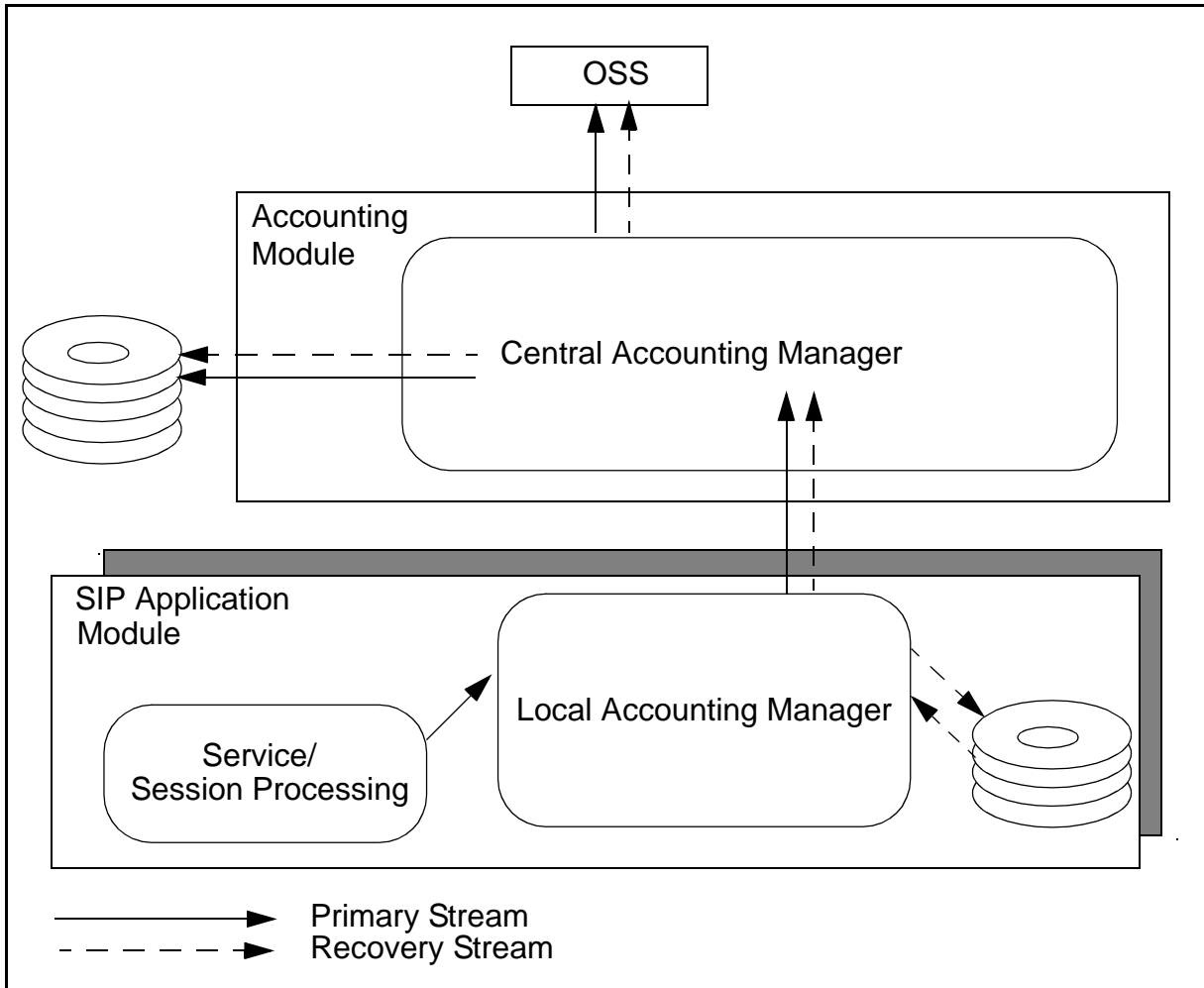
Strategy

The accounting module provides a framework that enables the transport of accounting information from the network to the back-end billing system of a service provider. The accounting system is comprised of two logically distinct entities:

- Local Accounting Manager (LAM), which resides on the SIP Application Module, and
- Central Accounting Manager (CAM) resides on the Accounting Module which can be on its own or on the same server as the standby Management Module.

The following sections provide a high-level overview of the LAM and CAM.

Figure 1 Accounting overview



Local Accounting Manager (LAM)

The primary function of the LAM is to collect, as specific events occur, raw accounting data from active sessions on the SIP Application Module and transport it to the CAM. The LAM transports raw accounting data to the CAM by way of two accounting streams—a primary stream and a recovery stream (see Figure 1, "Accounting overview").

The primary stream is used to transport accounting data in near real-time to the CAM. When an active session passes accounting data to the LAM, it is packaged and transported to the CAM through the primary stream. If the primary stream cannot transmit the accounting data quickly enough to the CAM (due to either communications problems between the LAM and the CAM or an exceedingly high traffic spike), then the LAM begins to store accounting data locally on disk.

The recovery stream will automatically begin to transfer that stored data to the CAM as a low priority background task once the LAM-CAM communication path has been restored. Data delivered by the recovery stream is not delivered in a near real-time fashion.

To ensure that no data is lost from the LAM to the CAM, the LAM retains a copy of all data sent to the CAM until it receives confirmation that the data has been successfully processed by the CAM. During extraneous periods of congestion, or extended communications outages, the LAM is able to store the accounting data to the local disk for later transport over the recovery stream. The LAM retains up to 24 hours worth of data.

Central Accounting Manager (CAM)

The CAM receives data from the LAM, reformats it, and stores it onto disk. The CAM sends an acknowledgement to the LAM for each block of successfully stored accounting data. When the CAM receives a block of accounting data from the LAM, it reformats the raw data received into the Internet Protocol Detail Record/Extensible Markup Language (IPDR/XML) accounting records. IPDR/XML accounting records are stored on disk, and may be optionally directed toward a downstream Operations Support System (OSS) through configuration of a near real-time TCP/IP connection and/or FTP connection (FTP push or FTP pull). The CAM can be configured to compress the files containing IPDR/XML accounting records for optimum storage.

The CAM can simultaneously receive accounting data from multiple LAMs. For each connected LAM, the CAM supports reception of both a primary and a recovery accounting data stream. In order to provide data integrity, the CAM will never delete accounting records.



CAUTION

Monitor the alarms.

It is the responsibility of the customer to remove old accounting data to make room for new data. There are threshold alarms that notify the user when running out of disk space.



**CAUTION**

There is one LAM per SIP Application Module. It is recommended that the network is configured so that every LAM in the network will deliver its data to the same CAM.

Hardware

The Accounting Module physically resides on a Sun Netra t 1400/1405. The D1000 disk array is used to provide redundant storage of the accounting data. The hardware required is detailed in Table 1, "Hardware details".

Table 1 Hardware details

Hardware	Details
<p>Server</p> 	<p>Sun Netra t 1400/t 1405 with the following hardware features:</p> <ul style="list-style-type: none"> • 4 440 Mhz CPUs • 4 GB RAM • 2 36 GB Disks • 20 GB 4mm DDS-4 Internal Tape Drive • 1 Quad Fast Ethernet (QFE) PCI card • 1 10x Internal DVD-ROM drive • 1 PCI dual differential Ultra SCSI Diff card • 1400 model is DC-powered; 1405 model is AC-powered
<p>Disk array</p> 	<p>Sun Netra st D1000 RAID array:</p> <ul style="list-style-type: none"> • 4 36 GB disks • Hot-swap disk drives

Software

Software update loads for the Accounting Module are covered in the upgrade section of this document.

Tools and utilities

Both the CAM and LAM are configured through the System Management Console which is the interface to the Management Module. The System Management Console is a Java-based user interface that runs on a PC and has a look and feel similar to that of Microsoft Windows Explorer.

CAM properties are configured within the Central Accounting Manager tab for the Accounting Module using the System Management Console. LAM properties are configured within the Local Accounting Manager tab for the SIP Application Module within the System Management Console.

Understanding accounting attributes and events**Recording Units**

As the LAM collects accounting information for events that occur during sessions, it stores the data in Recording Units (RUs).

RU Blocks

At the same time that the LAM collects new RUs, it also places queued RUs into RU Blocks to send to the CAM.

Data Transport Protocol

A socket-based TCP/IP communication protocol is used for transmitting collected accounting information from the LAM in the SIP Application Module to the CAM in the Accounting Module. It also provides the appropriate acknowledgement of receipt of the data from the CAM in the Accounting Module to the LAM in the SIP Application Module.

Figure 2, "LAM flow," on page 8 provides a graphical explanation of the LAM internal workings and Figure 3, "CAM flow," on page 8 provides a graphical explanation of the CAM internal workings.

Figure 2 LAM flow

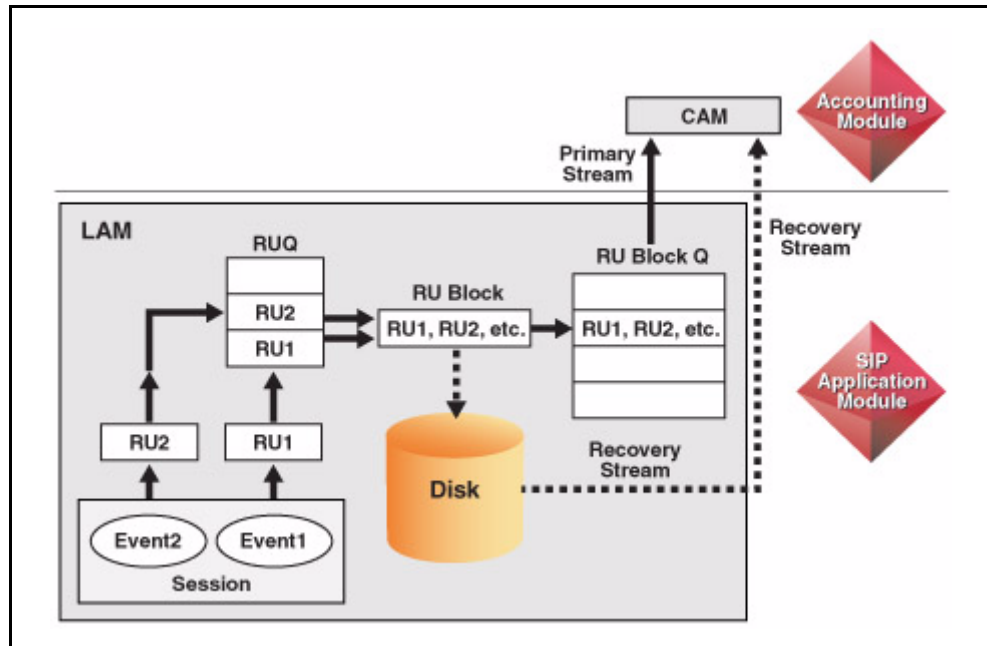
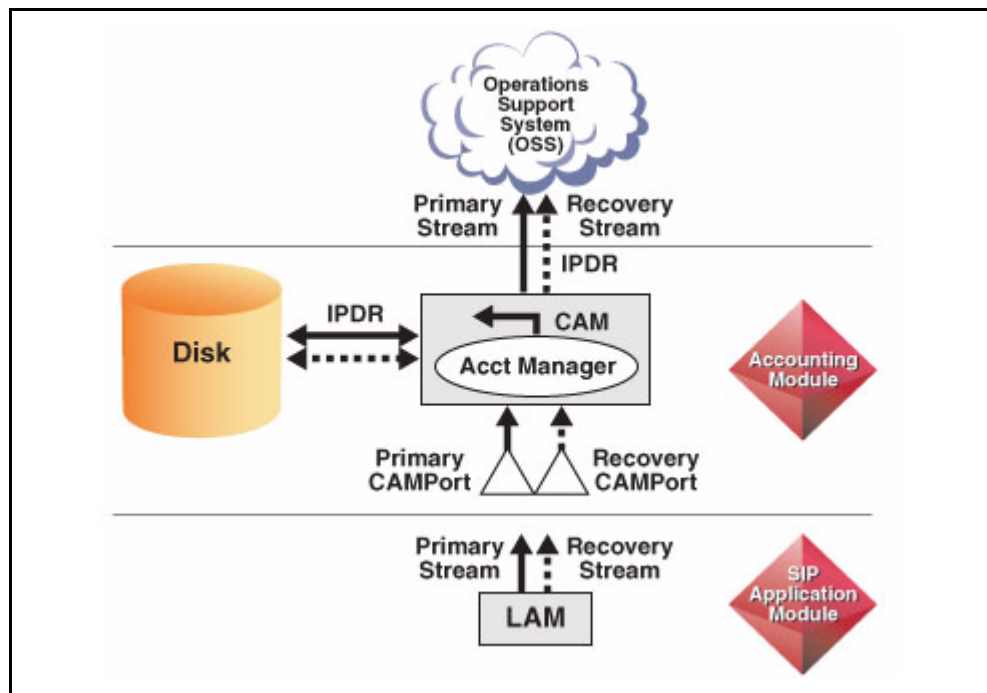


Figure 3 CAM flow



Service/Session Processing

Service/session processing collects raw accounting information in the SIP Application Module as specified events occur during a session. Service/session processing then passes this raw accounting information in the form of Recording Units (RUs) to the LAM for transport to the CAM. The LAM places the RUs into RU Blocks and transports the RU Blocks to the CAM. The transport mechanism used to transport RU Blocks from the LAM to the CAM is TCP/IP-based Data Transport Protocol. This near real-time data transfer constitutes the primary accounting stream from the LAM to the CAM.

If there is a loss of communication between the LAM and the CAM or an exceedingly high traffic spike, then RU Blocks are stored locally to disk on the LAM. Once communication between the LAM and the CAM is restored, the LAM resumes sending the RU Blocks along the primary accounting stream. Simultaneously, the RU Blocks that were previously stored on the LAM during the outage are sent along the recovery stream. The recovery accounting stream to the CAM has a lower priority than the primary accounting stream. The LAM stores up to 24 contiguous hours of raw accounting data in the event of communication loss to the CAM.

Note: This storage mechanism on the LAM is intended only as an emergency backup provision.

After the CAM acknowledges successful processing (receipt, translation and storage) of an RU Block, the LAM removes the corresponding copy of the RU Block at the LAM. This applies to both the Primary and Recovery streams.

Local file storage

When there is a communication loss from the LAM to the CAM and the local file storage that stores the RU Blocks is exceeded, a `diskAccessFailure` alarm is raised and all subsequent RUs are discarded.

There are two configurable alarm thresholds to warn of the onset of this condition. These thresholds determine the conditions for when the following alarms are raised:

- `DiskMonMajor` alarm - indicates when the local file storage is getting low.
- `DiskMonCritical` alarm - indicates when the local file storage is severely depleted.



Upgrades

How this chapter is organized

This chapter is organized as follows:

- “OAM&P strategy” on page 11
- “Task flows” on page 11
 - “Update a software load within a redundant network” on page 11
 - “Update a software load” on page 12

OAM&P strategy

This section describes the update strategy for the Accounting Module. The update has the following characteristics:

- does not impact stable calls.
- introduces new functionality.

Note: If an upgrade fails before or during the initial stages of the upgrade, the original version is restored and notification of the failure appears. If a component upgrade fails after the initial stages of the upgrade, it does not roll back automatically. A dialog box appears stating the upgrade failed and asks if you want to rollback.

Task flows

Update a software load within a redundant network

To prevent a loss of data, there are four basic steps that must be followed, in order, when updating a software load in a redundant network:

- 1 Update the standby instance of the Accounting Module. See “Update a software load” on page 12.
- 2 Perform a manual failover so that the standby instance of the Accounting Module becomes the “new” active instance of the Accounting Module. See “Failure strategy within a redundant network” on page 19 for the manual failover procedure.

- 3 Update the “old” active instance of the Accounting Module. See “Update a software load” on page 12.
- 4 Perform a manual failover so that the “old” active instance of the Accounting Module becomes the active instance. See “Failure strategy within a redundant network” on page 19 for the manual failover procedure.

Update a software load

The following procedure describes how to update a software load on the CAM:

Note 1: The LAM is updated along with the SIP Application Module. Refer to the *MCP SIP Application Module Basics*.

Note 2: Updates to System Components must be performed in a specific order. Refer to the *MCP Basics* for further information.

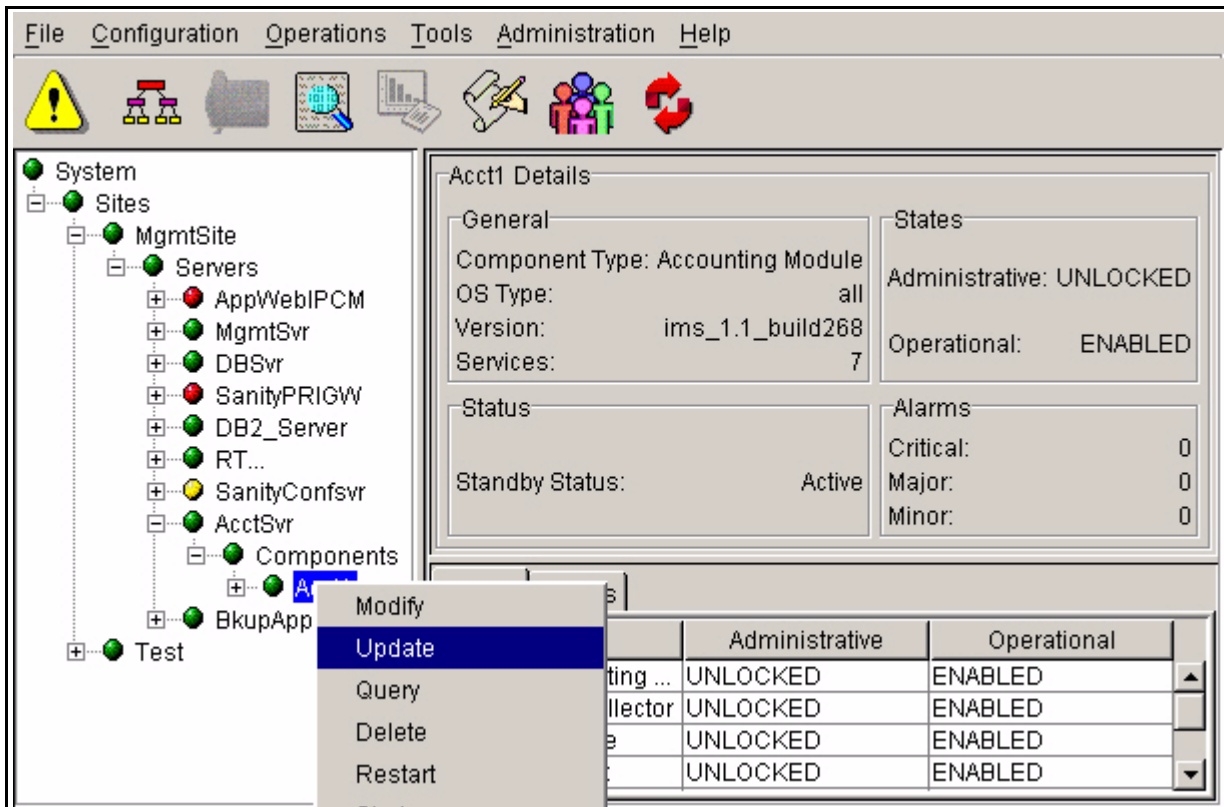
From the System Management Console

- 1 A load can be either up-versioned or down-versioned. In either case, updating a load from one version to another results in stopping and deleting the previously added version, adding the new version and auto-launching the new version. Therefore, there is no need to manually LOCK and UNLOCK the server. The steps involved in an update are described below.

From the System Management Console, under the Components folder, right-click on the Accounting Module.

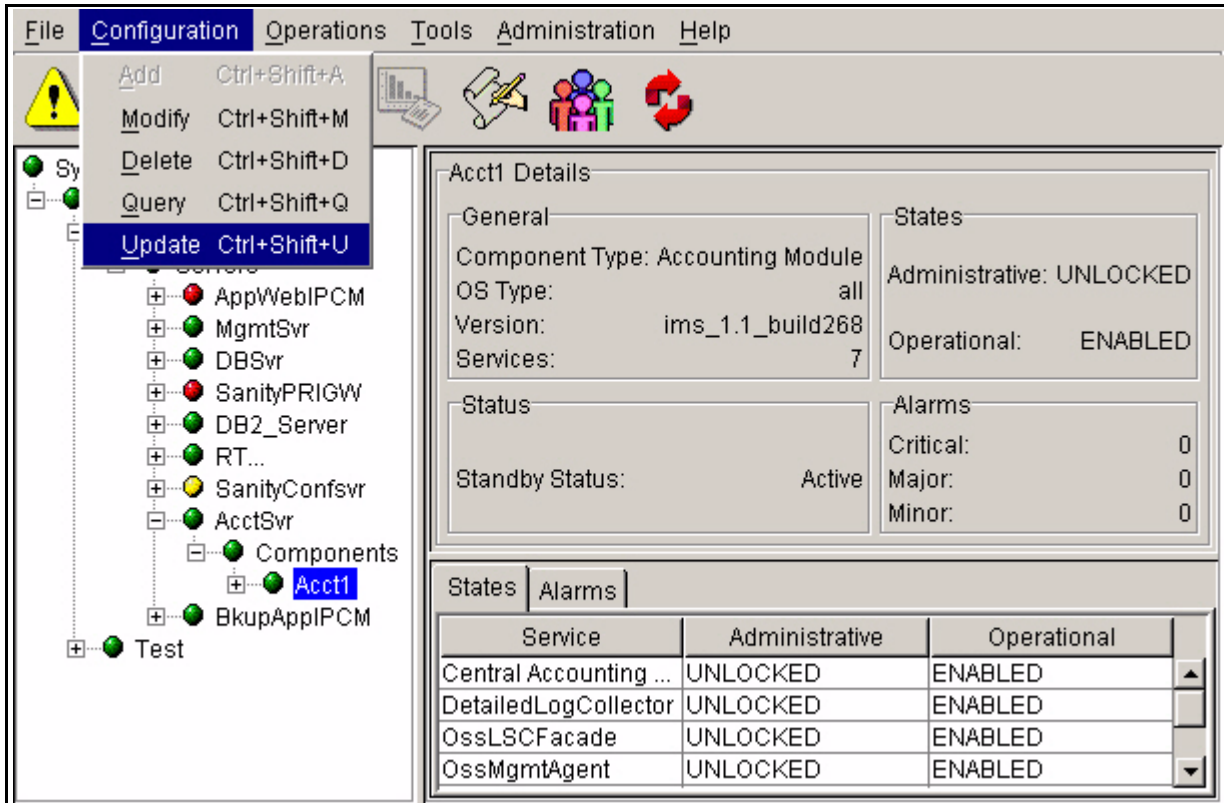
2 Select the **Update** command.

Figure 4 Updating the Accounting Module from the menu tree



You can also launch the update from the pull-down Configuration menu, as shown:

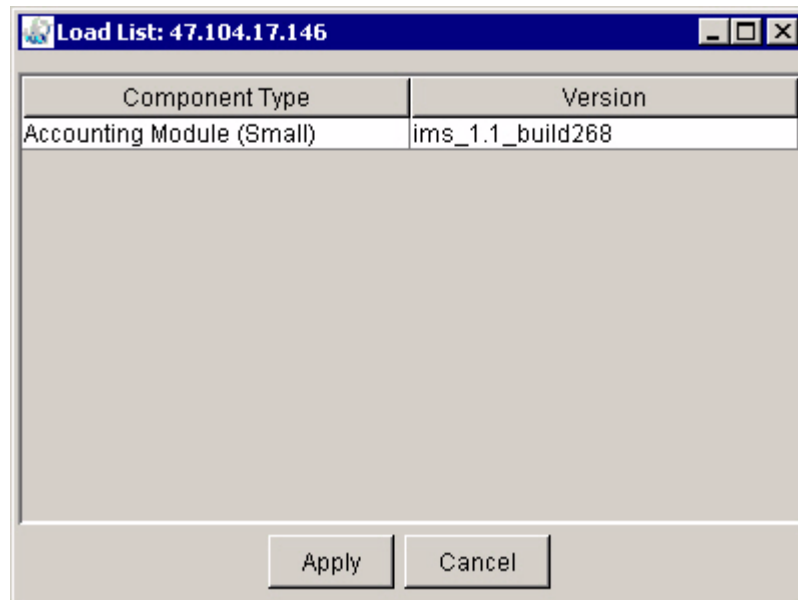
Figure 5 Updating the Accounting Module from the Configuration menu



3 After **Update** is selected, the following window appears:

Figure 6 The update window, retrieving the load list

- 4 The Load List window appears. The window only shows software loads intended for the Accounting Module component type, since this is the component type being updated.

Figure 7 Load list for updating

- 5 Select the load version that should be used to update the Accounting Module. Click on the **Apply** button.

- The System Management Console displays the Accounting Module configuration window with the CAM configuration properties.

Figure 8 Update CAM configuration tab

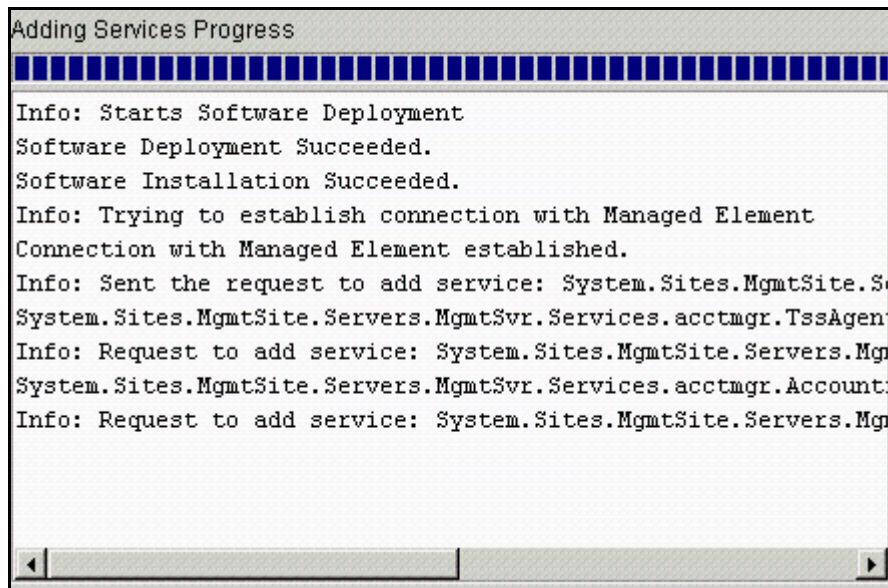
The screenshot shows the 'Central Accounting Manager' configuration window. The title bar reads 'Central Accounting Manager'. The window contains the following configuration fields:

CAM Mode :	SIP
* CAM IP Address :	47.104.17.153
* Primary CAM Port :	17667
* Recovery CAM Port :	17668
Base File Path :	/CAM/accounting
* File Rotation Size :	100000
* File Rotation Time :	20000
* File Compression :	<input type="checkbox"/>
* Disk Monitor Major Threshold :	50
* Disk Monitor Critical Threshold :	75
* TCP/IP Enabled :	<input type="checkbox"/>
TCP/IP IP Address :	0.0.0.0
TCP/IP Primary Host Port :	9000
TCP/IP Recovery Host Port :	9001
* FTP Push Enabled :	<input type="checkbox"/>
Primary FTP Directory :	
Recovery FTP Directory :	
Remote FTP Node ID :	0.0.0.0
FTP User ID :	
FTP USER Password :	

At the bottom right of the window is a 'Reset' button. Below the window are 'Apply' and 'Cancel' buttons.

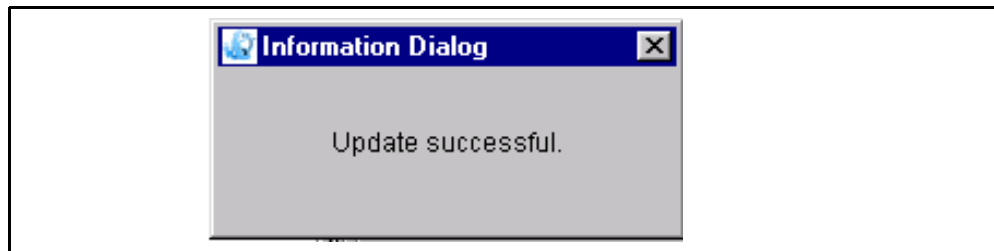
- If required, modify any configuration values. Click on the **Apply** button. The following window appears showing the progress of the update:

Figure 9 Progress of update



8 Once the update has completed, the following window appears:

Figure 10 Successful update dialog box





Fault management

How this chapter is organized

This chapter is organized as follows:

- “Network fault management strategy” on page 19
- “Failure strategy within a redundant network” on page 19
- “Failure strategy within a non-redundant network” on page 23

Network fault management strategy

The system handles network fault management through alarms and logs. Accounting alarms and logs occur on both the Local Accounting Manager and the Central Accounting Manager. Both CAM and LAM alarms and logs are viewed from the System Management Console. See the *MCP System Management Console Basics* for detailed information and tasks relating to accounting alarms and logs.

Failure strategy within a redundant network

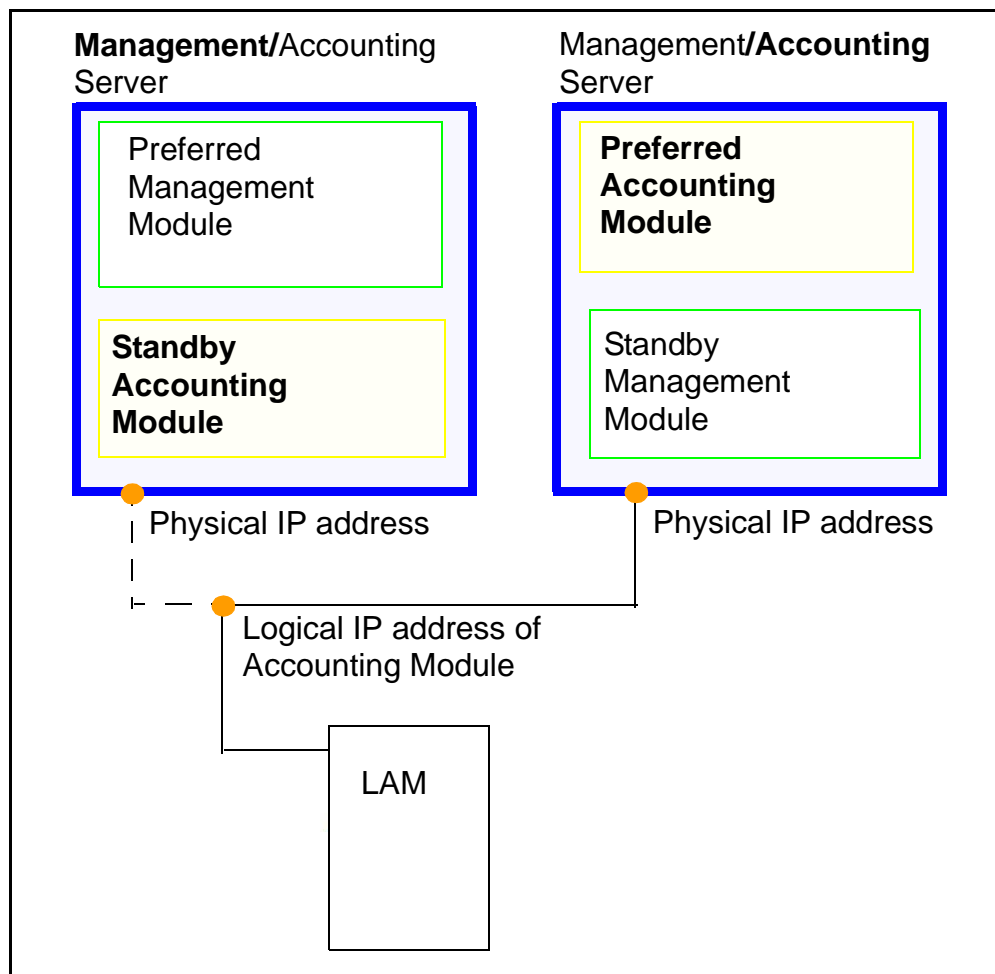
In a redundant network, there are two instances of the Accounting Module software present on two separate servers: one is designated as the preferred instance, and the other is designated as the standby. Additionally, these two servers are also configured to host two instances of the Management Module (again, as preferred/standby instances). These servers (termed the Management/Accounting servers) are configured so that one hosts the Preferred Management Module, and the other hosts the Preferred Accounting Module.

Manual failover of the Management/Accounting Module

Having two instances of the Accounting and Management Module software ensures the high availability of these two fundamental system components. If the server containing the Preferred Accounting Module fails, a manual failover allows the transfer of Accounting Module activity to the standby instance waiting on the server containing the Preferred Management Module. Similarly, if the server containing the Preferred Management Module fails, a manual failover allows the transfer of Management Module activity to the standby instance on the server containing the Preferred Accounting Module.

Both Accounting Module servers (the Preferred and Standby Accounting Module) have their own physical IP address. However, in order to provide a CAM failover mechanism that is transparent to the LAM (i.e. with no configuration changes), the concept of a logical IP address is used. The LAM is configured to connect to a logical IP address which is associated with the active instance of the CAM. This logical IP address identifies the active instance of the Accounting Module and is independent of a physical server, actually migrating from one physical server to the other as conditions dictate. During a manual failover, the logical IP address is updated in order to identify the new active instance after failover occurs. A logical view of this arrangement is shown in Figure 11, "Management/Accounting Server logical arrangement," on page 20.

Figure 11 Management/Accounting Server logical arrangement



If the Accounting Module (CAM) goes down, the LAM implicitly loses its connection to the CAM. In this case, the LAM will begin queuing

accounting information and (if the problem persists) storing accounting information to its local disk. To resolve this fault, an administrator needs to perform a manual failover to the Standby Accounting Module (installed on the Management/Accounting Server containing the Preferred Management Module). The manual failover process involves stopping the Preferred Accounting Module processes, releasing the associated logical IP address from the preferred module, and then on the Standby Module, stopping the process, assigning the logical IP address and restarting the process. These actions require the use of a Unix account to perform a remote login to the server.

Failover process

Failover for the Accounting Module is a manual process that should take only minutes to execute. For any failure, contact your next level of support to debug the root cause of the failure.

Failure of the Central Accounting Manager (CAM) will typically be indicated by alarms. There may also be alarms from one or more Local Accounting Managers (LAMs) executing on the SIP Application Module. Once it is determined that the active CAM is not responsive, switching to the standby is done as follows:

From the administrator workstation To stop the active Accounting Module:

- 1 If possible, establish a remote login session to what was the active Accounting Module. Login in as **sysadmin**.
Note: If it is not possible to establish a remote login session to the active Accounting Module, you still need to run the failover script as soon as connectivity to the Accounting Module is possible.
- 2 type: **cd /IMS/acctmgr/bin**
- 3 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl stop acctmgr**

This will ensure that the Accounting Module is placed in standby mode. If the process is still running it will be shut down, the logical IP will be unassigned and the process will be restarted. Since it is now in standby mode it will not receive data.

To start the standby Accounting Module:

- 4 Establish a remote login session to the standby Accounting Module. Login in as **sysadmin**.
- 5 type: **cd /IMS/acctmgr/bin**

- 6 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl start acctmgr**

The process will be stopped, the logical IP will be assigned for this machine and the Accounting Module process restarted. An example of the output from the script starting the Accounting Module is shown:

Example of the script starting the Accounting Module:

```
[@dev_pool31]/IMS/acctmgr/bin:=> sudo Failover.pl start acctmgr
Password:
> .
> killed
Created new logical interface qfe0:3
Logs are written to /IMS/acctmgr/SetActiveFlag.log
> .
> .
> .
>
> started
```

Output from ifconfig -a command is:

```
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232
    index 1 inet 127.0.0.1 netmask ff000000
qfe0: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,
    IPv4,NOFAILOVER> mtu 1500 index 2 inet 47.104.12.21 netmask fffff80
    broadcast 47.255.255.255 groupname imspub ether 8:0:20:ee:4d:5c
qfe0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
    index 2 inet 47.104.12.26 netmask fffff80 broadcast 47.255.255.255
qfe1: flags=79040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,
    IPv4,NOFAILOVER,FAILED,STANDBY,INACTIVE> mtu 1500 index 3
    inet 47.104.12.19 netmask fffff80 broadcast 47.255.255.255
    groupname imspub ether 8:0:20:ee:4d:5d
qfe2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
    index 6 inet 60.60.60.31 netmask ff000000 broadcast 60.255.255.255
    ether 8:0:20:ee:4d:5e
```

Logs are written to /tmp/Failover_acctmgr.log

```
[@dev_pool31]/IMS/acctmgr/bin:=>
```

Impacts and recovery

The Accounting Module is no longer running on the preferred server. If the active Accounting Module and the active Management Module are running on the same server, it may result in degraded capacity of the Accounting Module. To avoid any capacity problems, switch the active Accounting Module back to the preferred server as soon as it is available.

Restore to preferred server

Restoring the preferred Accounting Module to active status is basically the same process as failover. The main difference is that no failure has occurred.



CAUTION

This action will interrupt the communication link between the CAM and the LAM, forcing the LAM into a failure recovery mode of operation.

From the administrator workstation

To stop the active Accounting Module:

- 1 Establish a remote login session to the server on which the active accounting manager is running. Login in as **sysadmin**.
- 2 type: **cd /IMS/acctmgr/bin**
- 3 Use the sudo command to execute the failover script using the following syntax:

type: **sudo Failover.pl stop acctmgr**

The process will be shut down, the logical IP will be unassigned and the process will be restarted. It is now in standby mode and it will not receive data.

To start the standby Accounting Module:

- 4 Establish a remote login session to the other Accounting Manager (in this case the preferred one). Login in as **sysadmin**.
- 5 type: **cd /IMS/acctmgr/bin**
- 6 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl start acctmgr**

The process will be stopped, the logical IP will be assigned for this machine and the Accounting Manager process restarted.

Accessing accounting data on the standby accounting module

There should not be any changes to FTP access to accounting files on the Accounting Module when it is running in standby mode.

Failure strategy within a non-redundant network

In a non-redundant network, there is only one instance of the Accounting Module software present on a single server. Additionally, the same server is configured to host the instance of the Management

Module. If any failure occurs, it is recommended that your next level of support be contacted.



Configuration management

How this chapter is organized

This chapter is organized as follows:

- “Network strategy” on page 25
 - “Configuration procedures” on page 25

Network strategy

The network strategy is to configure all of the components in a central location. The central location for configuration is the System Management Console.

The following sections provide information on configuring the LAM and CAM.

Configuration procedures

Login to the System Management Console. For detailed procedures on logging into the System Management Console, please refer to the *MCP System Management Console Basics* document.

The CAM

Accounting Module properties are configured under the Central Accounting Manager tab on the Accounting Module within the System Management Console and cannot be modified in real-time.

The CAM is configured for:

- Data Transport Protocol
 - CAM IP address
 - Primary CAM port
 - Recovery CAM port
- file management
 - file rotation size
 - file rotation time
 - file compression
- disk full condition
 - disk monitor major threshold
 - disk monitor critical threshold
- TCP/IP transport to OSS
 - TCP/IP enabled
 - TCP/IP address
 - TCP/IP primary host port
 - TCP/IP recovery host port
- FTP transport to OSS
 - FTP push enabled
 - primary FTP directory
 - recovery FTP directory
 - remote FTP node ID
 - FTP user ID
 - FTP user password

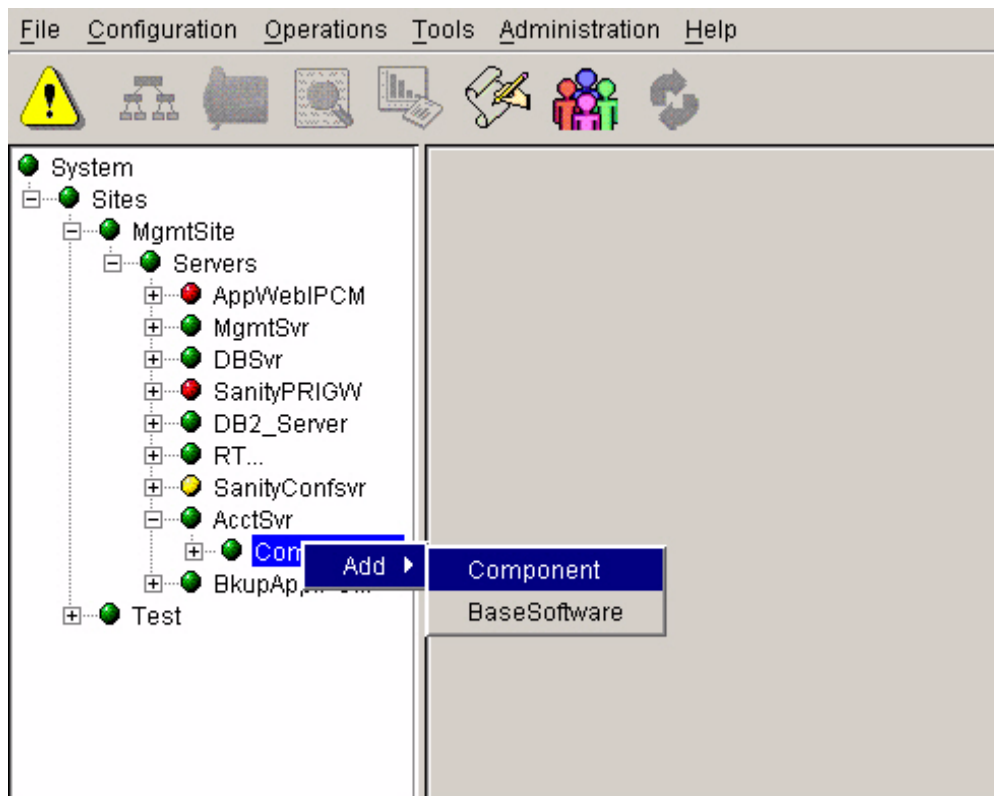
Adding the Accounting Module component

This procedure assumes that the Management/Accounting Server on which the Accounting Module component will be added has already been configured. For example, Figure 12, “Adding the component” shows the Accounting Module component being deployed onto the previously configured Management/Accounting Server.

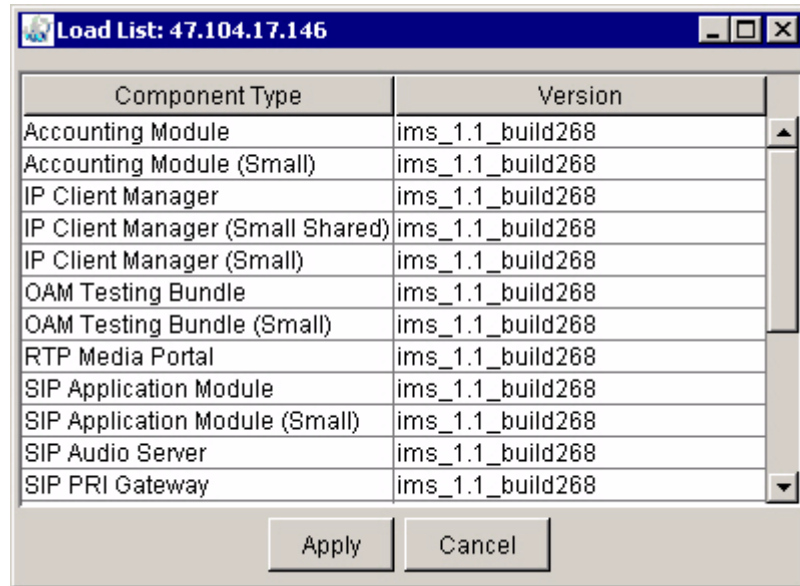
Note: In redundant networks, this procedure needs to be performed twice; once for the active instance of the Accounting Module and once for the standby instance of the Accounting Module.

From the System Management Console

- 1 Select the management server component from the system hierarchy as shown in Figure 12, “Adding the component”.
- 2 Right-click the highlighted word “Components” to get the option to add a component.
- 3 Select “Add” and then “Component”.

Figure 12 Adding the component

- 4 You will be prompted to choose a software load version.

Figure 13 Load list for adding

Component Type	Version
Accounting Module	ims_1.1_build268
Accounting Module (Small)	ims_1.1_build268
IP Client Manager	ims_1.1_build268
IP Client Manager (Small Shared)	ims_1.1_build268
IP Client Manager (Small)	ims_1.1_build268
OAM Testing Bundle	ims_1.1_build268
OAM Testing Bundle (Small)	ims_1.1_build268
RTP Media Portal	ims_1.1_build268
SIP Application Module	ims_1.1_build268
SIP Application Module (Small)	ims_1.1_build268
SIP Audio Server	ims_1.1_build268
SIP PRI Gateway	ims_1.1_build268

- 5 Select the desired software load version for the Accounting Module and click **Apply**.
- 6 You will be prompted to configure the CAM. See Figure 14 “CAM configuration tab,” on page 29.

Figure 14 CAM configuration tab

Central Accounting Manager

CAM Mode : SIP

* CAM IP Address : 0.0.0.0

* Primary CAM Port : 17667

* Recovery CAM Port : 17668

Base File Path : /CAM/accounting

* File Rotation Size : 100000

* File Rotation Time : 20000

* File Compression :

* Disk Monitor Major Threshold : 50

* Disk Monitor Critical Threshold : 75

* TCP/IP Enabled :

TCP/IP IP Address : 0.0.0.0

TCP/IP Primary Host Port : 9000

TCP/IP Recovery Host Port : 9001

* FTP Push Enabled :

Primary FTP Directory :

Recovery FTP Directory :

Remote FTP Node ID : 0.0.0.0

FTP User ID :

FTP USER Password :

Reset

Service Component Name:

Apply Cancel

The table below describes the configuration properties of the CAM:

Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
CAM mode	Type: String Range: SIP Default: SIP	Note: This field is not configurable.
CAM IP Address	Type: String Range: 1-15 characters Default: 0.0.0.0	The Logical IP address for the Accounting Module that would be written into the IPDR. Note: The default value must be updated in order for the functionality to work correctly.
Primary CAM Port	Type: Integer Range: 1025-65535 Default: 17667	Designates the network communications port number on the Accounting Module used by the Primary Stream. Note: The default value is recommended.
Recovery CAM Port	Type: Integer Range: 1025-65535 Default: 17668	Designates the network communications port number on the Accounting Module used by the Recovery Stream. Note: The default value is recommended.
Base File Path	Type: String Range: 1-500 characters Default: /CAM/accounting	Designates the path which further identifies where the formatted accounting files are stored on the Accounting Module. Note: This field is not configurable.

Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
File Rotation Size	Type: Integer (bytes) Range: 0 (disabled) 1-300000 Default: 100000	Designates the maximum file size allowable for accounting files to reach - after which file rotation takes place. A value of zero indicates no rotation based on file size. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.
File Rotation Time	Type: Integer (milliseconds) Range: 0 (disabled), 1-360000 (1 millisecond to 60 minutes) Default: 20000 (20 seconds)	Designates the maximum time interval for rotating accounting files from active to closed. A value of zero indicates no rotation based on time. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.
File Compression	Type: Boolean Range: True/False Default: False	Enables/disables compression of the IPDR formatted accounting information. The compressed files are stored with a ".zip" extension.

Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
Disk Monitor Major Threshold	Type: Integer Range: 0-100 Default: 50	Percentage of the accounting partition that can be used before a DiskMajorAlarm is raised. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
Disk Monitor Critical Threshold	Type: Integer Range: 0-100 Default: 75	Percentage of the accounting partition that can be used before a DiskCriticalAlarm is raised. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
TCP/IP Enabled	Type: Boolean Range: True/False Default: False	Enable/disable TCP/IP stream.
TCP/IP IP Address	Type: String Range: N/A Default: 0.0.0.0	Hostname or IP address of the destination server that will be receiving the TCP/IP stream. Note: The default value must be updated in order for the functionality to work correctly.
TCP/IP Primary Host Port	Type: Integer Range: 1025-65535 Default: 9000	The TCP port on the destination server that will receive the near-real-time flow for the Primary Stream accounting information.

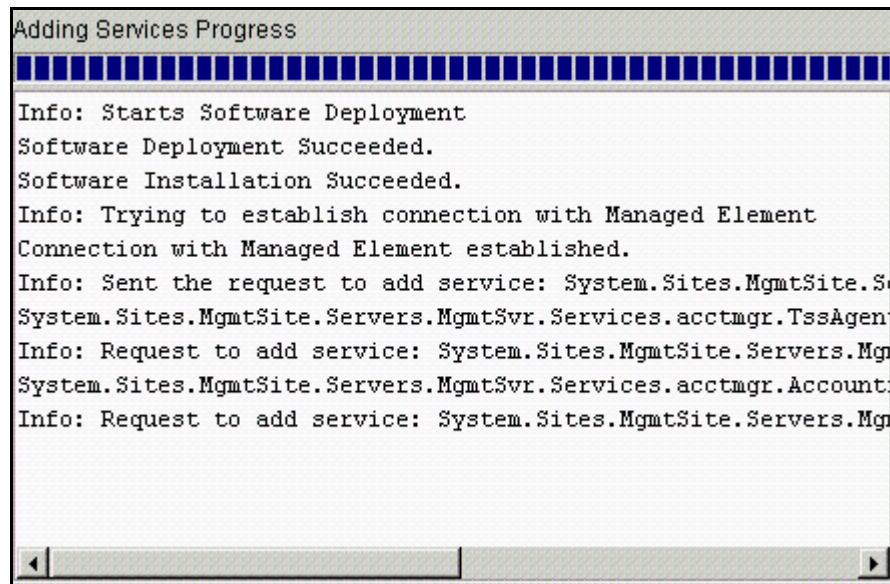
Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
TCP/IP Recovery Host Port	Type: Integer Range: 1025-65535 Default: 9001	The TCP port on the destination server that will receive the flow for the Recovery Stream accounting information.
FTP Push Enabled	Type: Boolean Range: True/False Default: False	Specifies whether or not automatic FTP transfer is enabled.
Primary FTP Directory	Type: String Range: 1-500 characters Default: N/A	Specifies the top-level directory on the remote FTP server where the IPDR files should be stored for the Primary Stream.
Recovery FTP Directory	Type: String Range: 1-500 characters Default: N/A	Specifies the top-level directory on the remote FTP server where the IPDR files should be stored for the Recovery Stream.
Remote FTP Node ID	Type: String Range: 1-500 characters Default: 0.0.0.0	Specifies the hostname for the destination server of the FTP stream. Note: The default value must be updated in order for the functionality to work correctly.
FTP User ID	Type: String Range: 1-500 characters Default: N/A	Specifies the login name for the remote host for FTP transfers.
FTP User Password	Type: String Range: 1-500 characters Default: N/A	Specifies the password used for FTP transfers.

- 7** After entering the appropriate configuration information, enter a label (six characters or less) in the Service Component Name Field. This label is the name that appears in the system

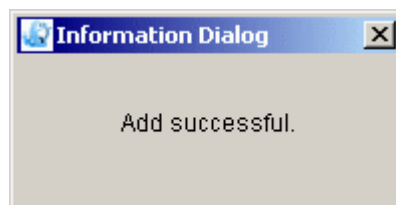
hierarchy tree. Click **Apply**. A progress screen appears while it deploys.

Figure 15 Adding Services Progress dialog box



- 8 When deployment completes, there is a screen showing that the component was added successfully.

Figure 16 The Add Successful dialog box



The LAM

Local Accounting Manager properties are configured under the Local Accounting Manager tab for the SIP Application Module within the System Management Console and cannot be modified in real-time. For further information, refer to the *MCP SIP Application Module Basics*.

The LAM is configured for:

- file management
 - file rotation size
 - file rotation time
- disk full conditions
 - disk monitor major threshold
 - disk monitor critical threshold

Configuring the LAM

When adding a SIP Application Module component, LAM configuration is required. For more details, refer to the *MCP SIP Application Module Basics*. Figure 17 “LAM configuration tab,” on page 35 shows the LAM configuration properties requiring configuration during the addition of a SIP Application Module component.

Figure 17 LAM configuration tab

The screenshot shows a configuration window titled "Local Accounting Manager". It contains several input fields for configuring LAM properties. The fields and their values are as follows:

Property	Value
* Primary CAM IP Address	47.104.17.146
* Primary CAM Port	17667
* Recovery CAM IP Address	47.104.17.150
* Recovery CAM Port	17668
Base File Path	/LAM/RUblock
* File Rotation Size	100000
* File Rotation Time	300
* Disk Monitor Major Threshold	50
* Disk Monitor Critical Threshold	75
RU Queue Size	2000
RUs Per Block	20
Block Rotation Time	1
RU Block Queue Size	1000

At the bottom right of the dialog is a "Reset" button. Below the dialog are "Apply" and "Cancel" buttons.

The LAM configuration properties are described in the following:

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
Primary CAM IP Address	Type: String Range: 1-15 characters Default: 0.0.0.0	Designates the logical IP address of the Primary Stream associated with the active Accounting Module. This is used to set up the connection for the Primary Stream between the Local Accounting Manager and the Central Accounting Manager. Note: The default value must be updated in order for the functionality to work correctly.
Primary CAM Port	Type: Integer Range: 1025-65535 Default: 17667	Designates the port number of the Accounting Module used to set up the connection for the Primary Stream between the Local Accounting Manager and the Central Accounting Manager.
Recovery CAM IP Address	Type: String Range: 1-15 characters Default: 0.0.0.0	Designates the logical IP address of the Recovery Stream associated with the active Accounting Module. This is used to set up the connection for the Recovery Stream between the Local Accounting Manager and the Central Accounting Manager. Note: The default value must be updated in order for the functionality to work correctly.
Recovery CAM Port	Type: Integer Range: 1025-65535 Default: 17668	Designates the port number of the Accounting Module used to set up the connection for the Recovery Stream between the Local Accounting Manager and the Central Accounting Manager.

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
Base File Path	Type: String Range: 1-500 characters Default: /LAM/RUblock	Designates the path which further identifies where the accounting files are stored on the SIP Application Module. If the directory is not created before the SIP Application Module software is added to the Server via the System Management Console, the Local Accounting Manager will create a new directory based on the file path specified in this property. Note: This field is not configurable.
File Rotation Size	Type: Integer (bytes) Range: 0-300000 Default: 100000	Specifies the maximum file size for the accounting file stored on the disk of the SIP Application Module. A value of zero indicates no rotation based on file size. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. This field is only used for the Recovery Stream. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
File Rotation Time	Type: Integer (seconds) Range: 0 (disabled), 1-3600 (1 second – 60 minutes) Default: 300 (5 minutes)	Designates the amount of time a file is writable. A value of zero indicates no rotation based on time. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. This field is only used for the Recovery Stream. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.
Disk Monitor Major Threshold	Type: Integer (percentage) Range: 1-100 Default: 50	Specifies the threshold of used disk space for the accounting disk partition when the Local Accounting Manager raises a DiskMajor alarm. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
Disk Monitor Critical Threshold	Type: Integer (percentage) Range: 1-100 Default: 75	Specifies the threshold of used disk space for the accounting disk partition when the Local Accounting Manager raises a DiskCritical alarm. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
RU Queue Size	Type: Integer (# of RUs) Range: 1-2000 Default: 2000	Specifies the maximum number of RUs stored within the RU queue. This parameter needs to be engineered based on real-time call capacity in order to provide optimum system performance. Note: This field is not configurable.

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
RUs Per Block	Type: Integer (# of RUs) Range: 1-20 Default: 20	Specifies the maximum number of RUs stored in an RU block to be transported from the Local Accounting Manager to the Central Accounting Manager. This parameter needs to be engineered based on real-time call capacity in order to provide optimum system performance. Note: This field is not configurable.
Block Rotation Time	Type: Integer (seconds) Range: 1-10 Default: 1	Specifies the maximum amount of time an RU Block is writable. This parameter needs to be engineered based on real-time call capacity in order to provide optimum system performance. Note: This field is not configurable.
RU Block Queue Size	Type: Integer (# of RU Blocks) Range: 1-1000 Default: 1000	Specifies the maximum number of RU Blocks stored within the RU Block Queue. This parameter needs to be engineered based on real-time call capacity in order to provide optimum system performance. WARNING! If the system fails, all data in the queue will be lost. Note: This field is not configurable.



Accounting management

How this chapter is organized

This chapter is organized as follows:

- “Accounting naming conventions” on page 41
 - “LAM output file directory” on page 41
 - “LAM recovery file naming convention” on page 42
 - “CAM output file directory” on page 42
 - “CAM file naming convention” on page 43
 - “Accessing accounting files on the CAM” on page 43
 - “Deleting accounting files on the CAM” on page 44
- “Accounting file format” on page 44
 - “General format” on page 44
 - “IPDR documents” on page 45
 - “IPDR elements and attributes” on page 52
- “Accounting record format” on page 53
 - “Record types” on page 53
 - “IPDR records” on page 54
 - “Element/Field definition” on page 67
 - “Record formats” on page 72
 - “Sample accounting records” on page 84

Accounting naming conventions

LAM output file directory

The directory where the RU Block file is located is:

```
/billing/LAM/RUblock/<AppModName>
```

where:

<AppModName> is the Component Name provided by the administrator when deploying the SIP Application Module through the System Management Console. For further information, refer to the *MCP SIP Application Module Basics*.

LAM recovery file naming convention

When writing recovery files to the directory structure built from the information in the previous section, the LAM uses the following file naming convention:

RUblocks_<date>@<time>.<extension>

where:

<date> is in <year><month><day> format

For example, 20010309 represents March 9, 2001

<time> is in <hours><minutes><seconds> <milliseconds> format

For example, 14170043 represents 14 hours 17 minutes 0 seconds and 43 milliseconds

<extension> is in one of the following strings:

- .active—represents an open RU Blocks file that is currently being written by the LAM
- .closed—represents a closed RU Blocks file that has been written, but has not yet been sent to the CAM
- .reading—represents an RU Blocks file that is currently being transferred to the CAM through the recovery stream

CAM output file directory

The actual directory containing the accounting information for the Primary Stream is:

/billing/CAM/accounting/Primary

and the directory for the Recovery Stream is:

/billing/CAM/accounting/Recovery

CAM file naming convention

When writing IPDR formatted files to the directory structure built from the information in the previous section, the CAM uses the following file naming convention:

```
IPDR_<date>@<time>.<extension>
```

where:

<date> is in <year><month><day> format

For example, 20010309 represents March 9, 2001

<time> is in <hours><minutes><seconds><milliseconds> format

For example, 14170043 represents 14 hours 17 minutes 0 seconds and 43 milliseconds

<extension> is in one of the following strings:

- .active—represents an open IPDR file that is currently being written by the CAM
- .closed—represents a closed RU file, which is available for retrieval by the OSS
- .closed.transferred—represents a transferred file via FTP Push (e.g. File has been sent via FTP to the customer OSS successfully).

Note: If compression is chosen, then the extensions would be .active and .closed.zip and .closed.zip.transferred.

Accessing accounting files on the CAM

To access files on the CAM, you need to establish a telnet session to the server:

From the telnet session

- 1 Establish a remote login session to the server. You will need a Login ID and Password. Contact your next level of support.
- 2 To access the Primary Stream directory on the CAM:
type: **cd /billing/CAM/accounting/Primary**
To access the Recovery Stream directory on the CAM:
type: **cd /billing/CAM/accounting/Recovery**
- 3 Type **ls** to see all the files in the directory.
- 4 To view a file:
type: **more <filename>**

- 5 To exit out of the session, type **exit**.

Deleting accounting files on the CAM



CAUTION

Ensure all information has been transferred to a back-end billing system prior to deletion.

It is recommended that the oldest files be deleted first.

To delete files on the CAM, you need to establish a telnet session to the server:

From the telnet session

- 1 Establish a remote login session to the server. You will need a Login ID and Password. Contact your next level of support.
- 2 To access the Primary Stream directory on the CAM:
type: **cd /billing/CAM/accounting/Primary**
To access the Recovery Stream directory on the CAM:
type: **cd /billing/CAM/accounting/Recovery**
- 3 Type **ls** to see all the files in the directory.
- 4 To delete a file:
type: **rm <filename>**
- 5 To exit out of the session, type **exit**.

Accounting file format

General format

In the Accounting Module, Extensible Markup Language (XML) is used to format accounting data into accounting records. XML is a standard created by the W3C (World Wide Web Consortium). It is a subset of SGML (Structured Generalized Markup Language), and is used to store data in a machine-independent way through the use of tags.

XML tags look similar to HTML (Hyper Text Markup Language) bracketed strings which delimit each piece of data. Each accounting field has a unique markup tag that allows any XML parser to recognize it.

XML was chosen due to its generic format, flexible structure, and human+machine readability. It serves the same purpose as arbitrarily formatted tags while adding the weight of a standard.

The XML format is based on Version 2.0 of the IPDR specification (“Network Data Management - Usage (NDM-U) For IP-Based Services”). The IPDR specification defines what is termed an IPDR document, which encompasses many IPDR records. An IPDR record, in turn, is also made up of categorized accounting information. This accounting information is categorized into a Service Session (SS) (composed of Service Consumer (SC) and Service Element (SE) information) and Usage Event (UE) information.

In this document, an IPDR document is synonymous to an accounting file; while IPDR records are synonymous to accounting records.

In order to describe the outputted XML format, Version 2.0 of the IPDR specification uses the XML Schema language defined by the W3C. The IPDR document is described using a Master Schema defined within the IPDR specification.

Service Schemas further define the IPDR document by defining the IPDR records within the document. Each type of service has a service schema associated with it which defines the accounting information that is captured in order to bill end-users (Service Consumers) for that service. The IPDR specification also provides schemas for some example services, including VoD (Video on Demand) and VoIP (Voice over IP).

Although the IPDR specification is in its infancy and requires expansion in some areas, it was chosen due to its ability to provide a good base and general standard for building accounting/detail records for IP-type services.

IPDR documents

When accounting records are written to a file, they are written in the form of IPDR documents. The format of the file is based on the structure laid out in the Master Schema. The following figures show the IPDR Master Schema:

Figure 18 IPDR Master Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c
http://www.w3.org/2001/XMLSchema-->
<schema xmlns="http://www.w3.org/2001/XMLSchema" targetName-
space="http://www.ipdr.org/namespaces/ipdr"
xmlns:ipdr="http://www.ipdr.org/namespaces/ipdr">
  <annotation>
    <documentation> This is the base type for the Service Consumer
      element. The service specific schema can extend
      this by deriving from it.
    </documentation>
    <documentation> This is the base type for the SE (Service
      Element)element. The service specific schema can extend
      this by deriving from it.
    </documentation>
    <documentation> This is the base type for the UE (Usage Entry)
      element. The service specific schema can extend
      this by deriving from it.
    </documentation>
  </annotation>
  <element name="IPDRDoc">
    <annotation>
      <documentation> The IPDRDoc element is the top-level container
        of a set of IPDRs. The document will also define the entity
        which recorded these IPDRs via the IPDRRec element.
      </documentation>
    </annotation>
    <complexType>
      <sequence>
        <element ref="ipdr:IPDRRec"/>
        <element ref="ipdr:IPDRRecList" minOccurs="0"/>
        <element ref="ipdr:IPDR" maxOccurs="unbounded"/>
        <element ref="ipdr:IPDRDoc.End" minOccurs="0"/>
      </sequence>
      <attribute name="seqNum" type="integer"/>
      <attribute name="version" type="string"/>
      <attribute name="startTime" type="dateTime"/>
      <attribute name="info" type="string"/>
    </complexType>
  </element>
</schema>

```

Figure 19 IPDR Master Schema, cont'd

```
</element>
<element name="IPDRDoc.End">
  <annotation>
    <documentation> The IPDRDoc.End element optionally marks the
      end of the IPDR block. It may contain some check
      information like a count of IPDRs.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="count" type="integer"/>
    <attribute name="endTime" type="dateTime"/>
  </complexType>
</element>
<element name="IPDRRec">
  <annotation>
    <documentation> The IPDRRec element describes the entity that
      is responsible for creating (recording) the IPDRDoc.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="id" type="ID"/>
    <attribute name="startTime" type="dateTime"/>
    <attribute name="info" type="string"/>
  </complexType>
</element>
<element name="IPDRRecRef">
  <annotation>
    <documentation> The IPDRRecRef element may be used to associate
      common references to the same IPDRRec element without
      repeating its other usage attributes.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
</element>
```

Figure 20 IPDR Master Schema, cont'd

```

<element name="IPDRRecList">
  <annotation>
    <documentation> The IPDRRecList identifies contributing IPDR
      recording entities which were used in the construction
      of the current IPDR Document. A typical example use
      would be for an aggregator of IPDR documents to
      identify the set of initial recorders presenting
      IPDRs.
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <element ref="ipdr:IPDRRec" maxOccurs="unbounded"/>
    </sequence>
  </complexType>
</element>
<element name="IPDR">
  <annotation>
    <documentation> An IPDR describes an event between a Service
      Consumer (SC) and a Service Element (SE). The SC and SE
      elements are contained beneath an entity called the
      Service Session (SS). Details of the event is contained
      in the Usage Entry (UE) element. All IPDRs have a time
      indicating when the event occurred.
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <choice minOccurs="0">
        <element ref="ipdr:IPDRRec"/>
        <element ref="ipdr:IPDRRecRef"/>
      </choice>
      <choice>
        <element ref="ipdr:SS"/>
        <element ref="ipdr:SSRef"/>
      </choice>
      <element ref="ipdr:UE"/>
      <element ref="ipdr:BaseIPDR" minOccurs="0"/>
    </sequence>
  </complexType>
</element>

```


Figure 21 IPDR Master Schema, cont'd

```

    <attribute name="id" type="ID"/>
    <attribute name="time" use="required" type="dateTime"/>
    <attribute name="seqNum" type="integer"/>
  </complexType>
</element>
<element name="SS">
  <annotation>
    <documentation> The Service Session (SS) element groups the
      Service Consumer and Service Element information. This
      grouping allows an SC/SE pair to be associated with other
      IPDRs via a single reference (the SSRef).
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <choice>
        <element ref="ipdr:SC"/>
        <element ref="ipdr:SCRef"/>
      </choice>
      <choice>
        <element ref="ipdr:SE"/>
        <element ref="ipdr:SERef"/>
      </choice>
    </sequence>
    <attribute name="id" type="ID"/>
    <attribute name="service" type="string"/>
  </complexType>
</element>
<complexType name="SCType" final="restriction">
  <sequence/>
  <attribute name="id" type="ID"/>
</complexType>
<element name="SC" type="ipdr:SCType">
  <annotation>
    <documentation> This element describes the Service Consumer.
  </documentation>
  </annotation>
</element>

```

Figure 22 IPDR Master Schema, cont'd

```

<complexType name="SEType" final="restriction">
  <sequence/>
  <attribute name="id" type="ID"/>
</complexType>
<element name="SE" type="ipdr:SEType">
  <annotation>
    <documentation> This element describes the Service Element.
  </documentation>
  </annotation>
</element>
<complexType name="UEType" final="restriction">
  <sequence/>
  <attribute name="type" default="Start-Stop">
    <simpleType>
      <restriction base="string">
        <enumeration value="Start"/>
        <enumeration value="Stop"/>
        <enumeration value="Start-Stop"/>
        <enumeration value="Interim"/>
      </restriction>
    </simpleType>
  </attribute>
</complexType>
<element name="UE" type="ipdr:UEType">
  <annotation>
    <documentation> This element describes the Usage Entry.
  </documentation>
  </annotation>
</element>
<element name="SSRef">
  <annotation>
    <documentation> The SSRef element may be used to associate common
      references to the same pairing of a Service Consumer
      and a Service Element.
  </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>

```

Figure 23 IPDR Master Schema, cont'd

```
</element>
<element name="SERef">
  <annotation>
    <documentation> The SERef element may be used to associate
      common references to the Service Element.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
</element>
<element name="SRef">
  <annotation>
    <documentation> The SRef element may be used to associate
      common references to the Service Consumer.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
</element>
<element name="BaseIPDR">
  <annotation>
    <documentation> The BaseIPDR element allows reference to be
      made to IPDRs which contributed to the construction of the
      current IPDR element.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="refs" use="required" type="IDREFS"/>
  </complexType>
</element>
</schema>
```

IPDR elements and attributes

Within the IPDR Master Schema, there are many elements, and attributes for these elements, defined. However, only a subset of these are actually used within the accounting file/IPDR document. This subset is shown in the following table:

Table 4 IPDR elements and attributes used

Element(s) Used	Element Located Within	Attribute(s) Used	Description
IPDRDoc	N/A (root element)	seqNum	Indicates the accounting file/IPDR document sequence number.
		version	Indicates the IPDR version and Accounting Module release used to create the accounting file/IPDR document.
IPDRRec	IPDRDoc	id	Identifies the Accounting Module producing the accounting file/IPDR document.
		startTime	Indicates the time when the accounting file/IPDR document was created.
IPDR	IPDRDoc	time	Indicates the time when the accounting/IPDR record was created in the file.
		seqNum	Indicates the accounting/IPDR record sequence number.
SS	IPDR	service	Indicates the type of the accounting/IPDR record.
SC	SS	N/A (none used)	N/A
SE	SS	N/A (none used)	N/A
UE	IPDR	N/A (none used)	N/A

Table 4 IPDR elements and attributes used

Element(s) Used	Element Located Within	Attribute(s) Used	Description
IPDRDoc.End	IPDRDoc	count	Indicates the number of accounting/IPDR records held within the accounting file/IPDR document.
		endTime	Indicates the time when the accounting file/IPDR document was closed.

Accounting record format

Record types

Accounting Records are produced based on events that occur during Service/Session processing. In response to these events, the following types of records are produced:

- Connect Ingress record - holds information regarding the setup/abandon/reject/answer portion of the session for the originating call model (OCM). This covers accounting for the following services: Authentication, Redirection, SDP (including Video, Collaboration, and CODEC information), Simultaneous Ringing, and Sequential Ringing.
- Connect Egress record - holds information regarding the setup/abandon/reject/answer portion of the terminating session for the terminating call model (TCM).
- Long Call Ingress - holds information regarding sessions for the OCM when a Long Call audit fails.
- Long Call Egress - holds information regarding sessions for the TCM when a Long Call audit fails.
- SDP record - holds SDP information which is received for the session during the middle of the call (between answer and disconnect). This covers accounting for the following services: Call Hold, Call Retrieve, and WebPush.
- REFER record - holds information regarding the transfer of calls during the middle of the call.
- Disconnect Ingress record - holds information regarding the disconnection of the session for the OCM.
- Disconnect Egress record - holds information regarding the disconnection of the session for the TCM.

For service diagrams and descriptions of call flows for the services encountered to produce these records, please refer to Appendix A of the *MCP SIP Application Module Basics*. This information is useful for understanding what events trigger the production of the accounting records as well as provide insight into the Method of Population for the majority of fields within the records.

IPDR records

The accounting record format is based on the VoIP (Voice over IP) service schema (which references the Master Schema) as defined within the IPDR specification. A schema (called NortelIMS_VoIPschema.xsd) has been developed based on the VoIP service schema in order to hold all of the Nortel accounting record information. The following figures show the current version of the Nortel Service Schema as of the release of this document:

Note: The latest Nortel Service Schema can be retrieved from the `\billing` directory on the server where the Accounting Module was deployed.

Figure 24 Nortel Service Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- <!DOCTYPE xs:schema SYSTEM "XMLSchema.dtd" [
  <!ENTITY % schemaAttrs "xmlns:ipdr CDATA #IMPLIED
                                xmlns:nortel CDATA #IMPLIED">
]> -->
<!--Generated by XML Authority. Conforms to w3c
http://www.w3.org/2001/XMLSchema-->
<xs:schema targetNamespace="http://www.nortelnetworks.com/namespaces/ipdr"
xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified"
xmlns:ipdr="http://www.ipdr.org/namespaces/ipdr"
xmlns:nortel="http://www.nortelnetworks.com/namespaces/ipdr">
  <xs:import namespace="http://www.ipdr.org/namespaces/ipdr" schemaLoca-
tion="ipdr2.0.xsd"/>
  <!-- Nortel types -->
  <xs:simpleType name="boolean">
    <xs:annotation>
      <xs:documentation>
        String enumeration for boolean true or false values.
      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="string">
      <xs:enumeration value="true"/>
      <xs:enumeration value="false"/>
    </xs:restriction>
  </xs:simpleType>
  <!-- Element definitions and documentation -->
  <xs:element name="corrID" type="string">
    <xs:annotation>
      <xs:documentation>
        The unique ID used to correlate ingress and egress accounting
        records within the IMS network.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

```

Figure 25 Nortel Service Schema, cont'd

```
<xs:element name="notifyArrival" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The time when the "NOTIFY" message is received during the call
      transfer.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="recTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The time the accounting information was captured at the SIP
      application server.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="uID" type="string">
  <xs:annotation>
    <xs:documentation>
      Identifies a session in the IMS network.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="referBy" type="string">
  <xs:annotation>
    <xs:documentation>
      The address of the party which transferred a session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="referTo" type="string">
  <xs:annotation>
    <xs:documentation>
      The address of the party to which a session is transferred.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```


Figure 26 Nortel Service Schema, cont'd

```
<xs:element name="referArrival" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The time the "REFER" message is received during a call transfer.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="referStatus" type="integer">
  <xs:annotation>
    <xs:documentation>
      This indicates if a successful "NOTIFY" message has been received
      for the "REFER" message during a transfer.
      0 is unknown status, 1 indicates a failure, 2 indicates success.
      No other values are valid.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="protocol" type="string">
  <xs:annotation>
    <xs:documentation>
      The session protocol used during the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="origDest" type="string">
  <xs:annotation>
    <xs:documentation>
      The first address the session was originally routed to.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="subscriberID" type="string">
  <xs:annotation>
    <xs:documentation>
      The SIP address of the originator for a session or a mid-call
      request.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 27 Nortel Service Schema, cont'd

```
<xs:element name="callingPSTN" type="string">
  <xs:annotation>
    <xs:documentation>
      The PSTN number for the calling party (originator) of the session.
    </xs:documentation>
    <xs:appinfo>
      Found in SC records only.
    </xs:appinfo>
  </xs:annotation>
</xs:element>
<xs:element name="oUA" type="string">
  <xs:annotation>
    <xs:documentation>
      The originating User Agent that was used for the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="startTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      When the SIP Application server received an initial "INVITE"
      request message issued by the originator.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="endTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      Indicates when a session has ended.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="destinationPhoneNumber" type="string">
  <xs:annotation>
    <xs:documentation>
      The SIP address of the terminator being attempted.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 28 Nortel Service Schema, cont'd

```
<xs:element name="proprietaryErrorCode" type="integer">
  <xs:annotation>
    <xs:documentation>
      The SIP response type when a failed session occurs.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="aband" type="nortel:boolean">
  <xs:annotation>
    <xs:documentation>
      Indicates if a call was abandoned before answering.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="ansInd" type="nortel:boolean">
  <xs:annotation>
    <xs:documentation>
      Indicates if a call was answered.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="webURI" type="string">
  <xs:annotation>
    <xs:documentation>
      The URI of the web page being pushed.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="tUA" type="string">
  <xs:annotation>
    <xs:documentation>
      The terminating user agent.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 29 Nortel Service Schema, cont'd

```
<xs:element name="tMG" type="string">
  <xs:annotation>
    <xs:documentation>
The terminating media gateway.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="oMG" type="string">
  <xs:annotation>
    <xs:documentation>
The originating media gateway.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="sdpPort" type="integer">
  <xs:annotation>
    <xs:documentation>
    The sdp port used in the media connection.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="sdpProtocol" type="string">
  <xs:annotation>
    <xs:documentation>
    The protocol used in the media connection.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="sessionName" type="string">
  <xs:annotation>
    <xs:documentation>
    The name of the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 30 Nortel Service Schema, cont'd

```
<!-- Media block elements -->
<xs:element name="succStatus" type="string">
  <xs:annotation>
    <xs:documentation>
      The success status.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="failRsn" type="string">
  <xs:annotation>
    <xs:documentation>
      The failure reason.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="fromAddr" type="string">
  <xs:annotation>
    <xs:documentation>
      The from address.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="fromPSTNnum" type="string">
  <xs:annotation>
    <xs:documentation>
      The PSTN number from which the call/action came.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="toAddr" type="string">
  <xs:annotation>
    <xs:documentation>
      The to address.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 31 Nortel Service Schema, cont'd

```
<xs:element name="attemptList" type="string">
  <xs:annotation>
    <xs:documentation>
      The list of addresses attempted for a SimRing or SeqRing request.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="connParty" type="string">
  <xs:annotation>
    <xs:documentation>
      The party connected to.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="phoneNo" type="string">
  <xs:annotation>
    <xs:documentation>
      The phone number used in the call.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="ansTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The date and time the call was answered.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="outpulsedDigits" type="string">
  <xs:annotation>
    <xs:documentation>
      The digits outpulsed to the gateway.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 32 Nortel Service Schema, cont'd

```

<xs:complexType name="SC-VoIP-Type">
  <xs:complexContent>
    <xs:extension base="ipdr:SCType">
      <xs:sequence>
        <xs:element name="subscriberID" type="string" minOccurs="0"/>
        <xs:element name="callingPSTN" type="string" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="SE-VoIP-Type">
  <xs:complexContent>
    <xs:extension base="ipdr:SEType">
      <xs:sequence>
        <xs:element name="appSrvID" type="string"/>
        <xs:element name="appSrvVer" type="string"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="Codec-List-Type">
  <xs:sequence>
    <xs:element name="codec" type="string" minOccurs="1" maxOc-
curs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="Media-List-Type">
  <xs:annotation>
    <xs:documentation>This describes the media block.</xs:documenta-
tion>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="mediaName" type="string"/>
    <xs:element name="sdpProtocol" type="string"/>
    <xs:element name="sdpPort" type="integer"/>
    <xs:element name="connAddr" type="string" minOccurs="0"/>
    <xs:element name="codecList" type="nortel:Codec-List-Type" minOc-
curs="0"/>
  </xs:sequence>

```

Figure 33 Nortel Service Schema, cont'd

```

</xs:complexType>
<!-- servType is an enumeration -->
<xs:simpleType name="Service-Type">
  <xs:annotation>
    <xs:documentation>Enumerate the valid service types.</xs:documenta-
tion>
  </xs:annotation>
  <xs:restriction base="string">
    <xs:enumeration value="SDP"/>
    <xs:enumeration value="SimRing"/>
    <xs:enumeration value="Authentication"/>
    <xs:enumeration value="SeqRing"/>
    <xs:enumeration value="Redirection"/>
    <xs:enumeration value="REFER"/>
  </xs:restriction>
</xs:simpleType>
<xs:complexType name="supplementaryService-Type">
  <xs:annotation>
    <xs:documentation>
      This is a superset of all the supplementaryService varieties that
      the IMS system can present.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="servType" type="nortel:Service-Type"/>
    <xs:element ref="nortel:corrID" minOccurs="0"/>
    <xs:element ref="nortel:referBy" minOccurs="0"/>
    <xs:element ref="nortel:referTo" minOccurs="0"/>
    <xs:element ref="nortel:referArrival" minOccurs="0"/>
    <xs:element ref="nortel:referStatus" minOccurs="0"/>
    <xs:element ref="nortel:subscriberID" minOccurs="0"/>
    <xs:element ref="nortel:succStatus" minOccurs="0"/>
    <xs:element ref="nortel:failRsn" minOccurs="0"/>
    <xs:element ref="nortel:fromAddr" minOccurs="0"/>
    <xs:element ref="nortel:fromPSTNnum" minOccurs="0"/>
    <xs:element ref="nortel:toAddr" minOccurs="0"/>
    <xs:element ref="nortel:attemptList" minOccurs="0"/>
    <xs:element ref="nortel:connParty" minOccurs="0"/>
    <xs:element ref="nortel:sessionName" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

```


Figure 34 Nortel Service Schema, cont'd

```

        <xs:element ref="nortel:phoneNo" minOccurs="0"/>
        <xs:element name="media" type="nortel:Media-List-Type" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<!-- UE group type -->
<xs:complexType name="UE-VoIP-Type">
    <xs:annotation>
        <xs:documentation>
            This is a superset of all the UE combinations.
        </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="ipdr:UEType">
            <xs:sequence>
                <xs:element ref="nortel:uID"/>
                <xs:element ref="nortel:corrID"/>
                <xs:element ref="nortel:recTime"/>
                <!-- all else are expressed as optional -->
                <xs:element ref="nortel:protocol" minOccurs="0"/>
                <xs:element ref="nortel:notifyArrival" minOccurs="0"/>
                <xs:element ref="nortel:startTime" minOccurs="0"/>
                <xs:element ref="nortel:endTime" minOccurs="0"/>
                <xs:element ref="nortel:tUA" minOccurs="0"/>
                <xs:element ref="nortel:tMG" minOccurs="0"/>
                <xs:element ref="nortel:oMG" minOccurs="0"/>
                <xs:element ref="nortel:ansTime" minOccurs="0"/>
                <xs:element ref="nortel:origDest" minOccurs="0"/>
                <xs:element ref="nortel:referBy" minOccurs="0"/>
                <xs:element ref="nortel:oUA" minOccurs="0"/>
                <xs:element ref="nortel:destinationPhoneNumber" minOccurs="0"/>
                <xs:element ref="nortel:proprietaryErrorCode" minOccurs="0"/>
                <xs:element ref="nortel:aband" minOccurs="0"/>
                <xs:element ref="nortel:ansInd" minOccurs="0"/>
                <xs:element ref="nortel:sessionName" minOccurs="0"/>
                <xs:element ref="nortel:phoneNo" minOccurs="0"/>
                <xs:element ref="nortel:webURI" minOccurs="0"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>

```

Figure 35 Nortel Service Schema, cont'd

```
        <xs:element name="media" type="nortel:Media-List-Type" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element ref="nortel:outpulsedDigits" minOccurs="0"/>
        <xs:element ref="nortel:failRsn" minOccurs="0"/>
        <xs:element ref="nortel:referTo" minOccurs="0"/>
        <xs:element ref="nortel:referArrival" minOccurs="0"/>
        <xs:element ref="nortel:referStatus" minOccurs="0"/>
        <xs:element name="supplementaryService" type="nortel:supplementaryService-Type" minOccurs="0" maxOccurs="5"/>
    </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:schema>
<!-- Local Variables: -->
<!-- mode:xml -->
<!-- End: -->
```

Element/Field definition

The following table lists the elements and fields used in the IPDR records:

Table 5 Element/Field list

Field Name	XML tag	Record Type	Element Found Within	Description
Answer Indicator	ansInd	ConnectIngress, ConnectEgress	UE	Indicates whether the call was answered.
Answer Time	ansTime	ConnectIngress, ConnectEgress	UE	If the call was answered, indicates the time of answer (in GMT).
Application Server ID	appSrvID	ALL	SE	Indicates the SIP Application Module which is producing the accounting record.
Application Server Version	appSrvVer	ALL	SE	Indicates the software Load Version of the SIP Application Module producing the accounting record.
Attempt List	attemptList	ConnectIngress	Supplementary Service	Indicates the addresses which were attempted for simultaneous ringing or sequential ringing.
Call Abandoned	aband	ConnectIngress, ConnectEgress	UE	Indicates whether the call was abandoned before the call was answered.
Calling Party PSTN Number	callingPSTN	ConnectIngress, ConnectEgress	SC	Indicates the PSTN number for the calling party (originator) of the session.
CODEC	codec	ConnectIngress, SDP	codecList	Indicates the CODEC chosen based on negotiation with the terminator.

Table 5 Element/Field list

Field Name	XML tag	Record Type	Element Found Within	Description
CODEC List	codecList	ConnectIngress, SDP	media	Contains a list of CODEC(s).
Connected Party	connParty	ConnectIngress	SupplementaryService	Indicates the address for the party that a session was finally connected to for the SimRing and SeqRing services.
Connection Address	connAddr	ConnectIngress, SDP	media	When set to 0.0.0.0, it indicates a session is on hold. Otherwise, it indicates the address of the terminating party.
Correlation ID	corrID	ALL	UE	Indicates a unique ID used to correlate ingress and egress accounting records within the network. This correlation ID can also be used to correlate accounting records with accounting records from the CS 2000 network.
Destination Phone Number	destinationPhoneNumber	ConnectIngress	UE	Indicates the address of the terminator being attempted.
End Time	endTime	ConnectIngress, ConnectEgress, DisconnectIngress, DisconnectEgress	UE	Indicates the time (in GMT) when a session has ended, either based on disconnection, abandonment or error.

Table 5 Element/Field list

Field Name	XML tag	Record Type	Element Found Within	Description
Failure Reason	failRsn	ConnectIngress, LongCallIngress, LongCallEgress	SupplementaryService; UE	Indicates the reason a failure has occurred (either during authentication or a long call audit).
Media	media	ConnectIngress, SDP	SupplementaryService; UE	Contains other elements/fields which provide information regarding a negotiated media during the session.
Media Name	mediaName	ConnectIngress, SDP	media	Indicates the type of media being transported during the session (i.e. audio, video).
Notify Arrival Time	notifyArrival	REFER	UE	Indicates the time (in GMT) the "NOTIFY" message is received during a call transfer.
Original Destination Address	origDest	ConnectIngress	UE	Indicates the first address the session was originally routed to.
Originating User Agent	oUA	ConnectIngress	UE	Identifies the originating User Agent that was used for the session.
Outpulsed Digits	outpulsed Digits	ConnectEgress	UE	Indicates the terminator's address, which is used to route the call on the outbound side of the session.

Table 5 Element/Field list

Field Name	XML tag	Record Type	Element Found Within	Description
Phone Number	phoneNo	ConnectIngress, SDP	SupplementaryService;UE	Indicates the phone number associated with the SDP sent during the session initiation. In the case of WebPush, it indicates that a WebPush was performed.
Proprietary Error Code	proprietaryErrorCode	ConnectIngress, ConnectEgress, DisconnectIngress, DisconnectEgress	UE	Indicates the SIP response type when a failed session occurs.
Protocol	protocol	ConnectIngress, ConnectEgress	UE	Indicates the protocol (SIP) that was used during the session.
Record Time	recTime	ALL	UE	Indicates the time (in GMT) an accounting record is produced at the SIP Application Module.
Redirected to Party Address	toAddr	ConnectIngress	SupplementaryService	Indicates the address of the party to which a session is redirected.
Redirecting Party Address	fromAddr	ConnectIngress	SupplementaryService	Indicates the address of the party which redirected a session.
Redirecting Party PSTN Number	fromPSTN	ConnectIngress	SupplementaryService	Indicates the PSTN number of the redirecting party for the session.

Table 5 Element/Field list

Field Name	XML tag	Record Type	Element Found Within	Description
Refer Arrival Time	referArrival	REFER	UE	Indicates the time (in GMT) when the request to transfer the call is received by the party being transferred.
Refer Status	referStatus	REFER	UE	Indicates if the call transfer was successful.
Refer to	referTo	REFER	UE	Indicates the address of the party to which a session is transferred.
Referred by	referBy	ConnectIngress, REFER	UE	Indicates the address of the party which transferred a session.
SDP Port	sdpPort	ConnectIngress, SDP	media	Indicates the port which was used to transport the media for the session.
SDP Protocol	sdpProtocol	ConnectIngress, SDP	media	Indicates the protocol used to transport the media for the session.
Service Type	servType	ConnectIngress	SupplementaryService	Indicates the type of service information captured within the SupplementaryService element (i.e. Authentication, Redirection, SDP, SimRing, SeqRing).
Session Name	sessionName	ConnectIngress, SDP	SupplementaryService;UE	Indicates the session name. In the case of collaboration, it indicates that it is a collaboration session.

Table 5 Element/Field list

Field Name	XML tag	Record Type	Element Found Within	Description
Start Time	startTime	ConnectIngress, ConnectEgress	UE	Indicates the time (in GMT) when the session begins.
Subscriber ID	subscriberID	ConnectIngress, SDP	SC	Indicates the SIP address of the originator for a session or a mid-call request.
Success Status	succStatus	ConnectIngress	SupplementaryService	Indicates whether authentication was successful.
Supplementary Service	supplementaryService	ConnectIngress	UE	Contains other elements/fields which provide information regarding a service provided during a session.
Terminating Media Gateway	tMG	ConnectEgress	UE	Identifies the terminating Media Gateway that was used for the session.
Terminating User Agent	tUA	ConnectEgress	UE	Identifies the terminating user agent for the session.
Unique Session Identifier	uID	ALL	UE	Identifies a session in the network.
Web URI Indicator	webURI	SDP	UE	Indicates the URI which was specified as part of the WebPush service.

Record formats

In order to provide a different layout of the accounting record information, each record and its fields are detailed. The “Method of Population” information for each field is provided as insight into the values that are recorded in each field. Since the majority of the

accounting information is gathered from the SIP messaging used during session processing, it is recommended that the SIP Draft RFC 2543 (see note for specific reference) be referenced for more information. However,

Note 1: J. Rosenberg et al, SIP: Session Initiation Protocol, Internet Draft draft-ietf-sip-rfc2543-bis09.txt, IETF, Feb 27, 2002.

Note 2: Your next level of support should be contacted regarding third party interoperability prior to implementing the SIP Draft RFC 2543 specification.

The following table lists the ConnectIngress record fields:

Table 6 ConnectIngress record fields

Field Name	Method of Population
Answer Indicator	Set when the SIP Application Module receives a "200 OK" Response message from the callee after the originator issued the "INVITE" Request message.
Answer Time	Based on a timestamp taken when the Originating Call Model (OCM) of the SIP Application Module receives a "200 OK" response message from the callee after the originator issued the "INVITE" request message.
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Call Abandoned	Set by the SIP Application Module when the call was cancelled without the call being answered.
Calling Party PSTN Number	Taken from the Remote-Party-ID header in the "INVITE" Request message from a PSTN.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
Destination Phone Number	Taken from the URL in the initial "INVITE" Request message issued by the originator.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Original Destination Address	Taken from the addr-spec portion of "TO" field in the initial "INVITE" Request message issued by the originator.
End Time	Based on the timestamp taken when a call is abandoned or an internal failure occurs.
Originating User Agent	Taken from the "User-Agent" header of the "INVITE" Request message received by the SIP Application Module.
Proprietary Error Code	Derived from various response messages received by the SIP Application Module when a session failed.
Protocol	Based on the protocol used to initiate the session.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Referred by	Taken from the "Referred-By" header of the "INVITE" message received when the transferred call is initiated.
Start Time	Based on a timestamp taken when an Initial "INVITE" Request message is received for the OCM by the SIP Application Module.
Subscriber ID	Taken from the addr-spec portion of "FROM" field in the initial "INVITE" Request message issued by the originator.
Supplementary Service: Authentication (servType)	<p>Contains information/elements regarding authentication. This information includes:</p> <ul style="list-style-type: none"> • Service Type - Indicates the type of service. In this case, it is Authentication. • Success Status - Indicates if authentication for the "INVITE" was successful or not. • Failure Reason - Based on the signal "407 Authentication Required" in response to the original "INVITE" issued by the originator.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Supplementary Service: Redirection (servType)	<p>Contains information/elements regarding redirection. This information includes:</p> <ul style="list-style-type: none">• Service Type - Indicates the type of service. In this case, it is Redirection.• Redirecting Party Address - Taken from the "200 OK" message received when the call is answered after being redirected to one or more parties.• Redirecting Party PSTN Number - Determined based on provisioning of the subscriber data field "Public Charge ID" in the Provisioning Client for the Redirecting Party Address.• Redirected to Party Address - Taken from the "200 OK" message received when the call is answered after being redirected to one or more parties.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Supplementary Service: SDP (servType)	<p>Contains information/elements regarding SDP. This information includes:</p> <ul style="list-style-type: none"> • Service Type - Indicates the type of service. In this case, it is SDP. • Media - contains information/elements regarding the media. This information includes: <ul style="list-style-type: none"> — CODEC List - contains a list of CODEC(s) as follows: <ul style="list-style-type: none"> – CODEC - Based on a portion of the media attributes field (a=) within the SDP header of the "INVITE" message. – Connection Address - Based on a portion of the connection data field (c=) within the SDP header of the "INVITE" message. – Media Name - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. – SDP Port - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. – SDP Protocol - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. • Phone Number - Based on a portion of the phone number field (p=) within the SDP header of the "INVITE" message. • Session Name - Based on a portion of the session name field (s=) within the SDP header of the "INVITE" message.
Supplementary Service: SimRing (servType)	<p>Contains information/elements regarding simultaneous ringing. This information includes:</p> <ul style="list-style-type: none"> • Attempt List - Based on user provisioning and client registrations. • Connected Party - Indicates the URL of the party who answers the session. It will match one of the parties in the Attempt List. • Service Type - Indicates the type of service. In this case, it is SimRing.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Supplementary Service: SeqRing (servType)	Contains information/elements regarding sequential ringing. This information includes: <ul style="list-style-type: none"> • Attempt List - Based on user provisioning and client registrations. • Connected Party - Indicates the URL of the party who answers the session. It will match one of the parties in the Attempt List. • Service Type - Indicates the type of service. In this case it is SeqRing.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the ConnectEgress record fields:

Table 7 ConnectEgress record fields

Field Name	Method of Population
Answer Indicator	Set when the SIP Application Module receives a "200 OK" Response message from the callee after the originator issued the "INVITE" Request message.
Answer Time	Based on a timestamp taken when the Terminating Call Model (TCM) of the SIP Application Module receives a "200 OK" response message from the callee after the originator issued the "INVITE" request message.
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Call Abandoned	Set by the SIP Application Module when the call was cancelled without the call being answered.
Calling Party PSTN Number	Taken from the Remote-Party-ID header in the initial "INVITE" Request message from a PSTN.

Table 7 ConnectEgress record fields

Field Name	Method of Population
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on the timestamp taken when a call is abandoned or an internal failure occurs.
Outpulsed Digits	Determined during Session Processing, it is the SIP address specified in the translated request URI field of the outgoing "INVITE" message from the SIP Application Module.
Proprietary Error Code	Derived from various response messages received by the Application Module when a session failed.
Protocol	Based on the protocol used to terminate the session.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Start Time	Based on a timestamp taken when an Initial "INVITE" Request message is received for the TCM by the SIP Application Module.
Terminating Media Gateway	Taken from the translated request URI field of the forwarding message sent by the SIP Application Module.
Terminating User Agent	Taken from the "User-Agent" header of the terminator's 200/OK message.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the LongCallIngress record fields:

Table 8 LongCallIngress record fields

Field Name	Method of Population
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on a timestamp taken when the Long Call audit determines that a call should be taken down.
Failure Reason	Error code given by the Long Call audit when it has been determined that a call should be taken down.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the LongCallEgress record fields:

Table 9 LongCallEgress record fields

Field Name	Method of Population
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.

Table 9 LongCallEgress record fields

Field Name	Method of Population
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on a timestamp taken when the Long Call audit determines that a call should be taken down.
Failure Reason	Error code given by the Long Call audit when it has been determined that a call should be taken down.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the SDP record fields:

Table 10 SDP record fields

Field Name	Method of Population
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.

Table 10 SDP record fields

Field Name	Method of Population
Media	<p>Contains information/elements regarding a negotiated media. This information includes:</p> <ul style="list-style-type: none"> • CODEC List - contains a list of CODEC(s) as follows: <ul style="list-style-type: none"> — CODEC - Based on a portion of the media attributes field (a=) within the SDP header of the "INVITE" message. • Connection Address - Based on a portion of the connection data field (c=) within the SDP header of the "INVITE" message. When the value is set to 0.0.0.0, it indicates the session is on hold. Otherwise, it indicates the address of the terminating party. • Media Name - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. • SDP Port - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. • SDP Protocol - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message.
Phone Number	<p>Based on a portion of the phone number field (p=) within the SDP header of the "INVITE" message. In the case of WebPush, it indicates that a WebPush was performed.</p>
Record Time	<p>Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).</p>
Session Name	<p>Based on a portion of the session name field (s=) within the SDP header of the "INVITE" message.</p>
Subscriber ID	<p>Taken from the addr-spec portion of "FROM" field in the "INVITE" message.</p>
Unique Session Identifier	<p>Taken from the "Call-ID" field in the "INVITE" message issued by the originator.</p>
Web URI	<p>Based on a portion of the web URI field (w=) within the SDP header of the "INFO" message.</p>

The following table lists the REFER record fields:

Table 11 REFER record fields

Field Name	Method of Population
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
Notify Arrival Time	Based on a timestamp taken when the "NOTIFY" message is received by the SIP Application Module during a call transfer.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Referred by	Taken from the "Referred-By" header of the "REFER" message received during a call transfer.
Refer Status	Based on whether a successful "NOTIFY" is received for a "REFER" message during a call transfer.
Refer to	Taken from the "Refer-To" header of the "REFER" message received during a call transfer.
Refer Arrival Time	Based on a timestamp taken when the "REFER" message is received by the SIP Application Module during a call transfer.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the DisconnectIngress record fields:

Table 12 DisconnectIngress record fields

Field Name	Method of Population
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on the timestamp taken when a "BYE" message is received by the Originating Call Module (OCM) of the SIP Application Module or when an internal failure occurs.
Proprietary Error Code	Derived from various response messages received by the SIP Application Module when a session failed.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the DisconnectEgress record fields:

Table 13 DisconnectEgress record fields

Field Name	Method of Population
Application Server ID	Based on the Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during deployment of the SIP Application Module.

Table 13 DisconnectEgress record fields

Field Name	Method of Population
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on the timestamp taken when a "BYE" message is received by the Terminating Call Model (TCM) of the SIP Application Module or when an internal failure occurs.
Proprietary Error Code	Derived from various response messages received by the SIP Application Module when a session failed.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

Sample accounting records

The following figures provide sample accounting records for the record types described in Section "Record types," on page 53 and the common billable services provided by the SIP Application Module. These accounting records are the current samples as of the release of this document.

Note: The latest sample accounting records can be retrieved from the `\billing\Sample` directory on the server where the Accounting Module was deployed.

Figure 36 Connect Ingress Record for Sequential Ringing

```

<ipdr:IPDR seqNum="22" time="2003-03-12T15:59:00Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>8080@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>532069808@lab2.org</uID>
    <corrID>532069808@lab2.org</corrID>
    <recTime>2003-03-12T15:58:46.81Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-12T15:58:44.43Z</startTime>
    <ansTime>2003-03-12T15:58:46.81Z</ansTime>
    <origDest>8081@lab2.org</origDest>
    <oUA>IMS1.1 Networks FP1 IP Nortel RAIDer/1.1.64</oUA>
    <destinationPhoneNumber>8081@lab2.org</destinationPhoneNumber>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>nortelnetworks</sessionName>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <sdpPort>54040</sdpPort>
        <connAddr>47.104.12.226</connAddr>
        <codecList>
          <codec>18 G729/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 37 Connect Ingress Record for Sequential Ringing, cont'd

```
<supplementaryService>
  <servType>SeqRing</servType>
  <attemptList>sip:8081@lab2.org:5070;maddr=47.104.12.148</attemptList>
  <connParty>sip:8081@lab2.org:5070;maddr=47.104.12.148</connParty>
</supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 38 Connect Ingress Record for Simultaneous Ringing

```

<ipdr:IPDR seqNum="82" time="2003-03-13T10:02:57Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>5089@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>6c04eae4_f3e81f0ald@test2_ipcmweb</uID>
    <corrID>6c04eae4_f3e81f0ald@test2_ipcmweb</corrID>
    <recTime>2003-03-13T10:02:42.34Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-13T10:02:34.50Z</startTime>
    <ansTime>2003-03-13T10:02:42.34Z</ansTime>
    <origDest>8080@lab2.org</origDest>
    <destinationPhoneNumber>8080@lab2.org</destinationPhoneNumber>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>Nortel Networks</sessionName>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <sdpPort>59224</sdpPort>
        <connAddr>47.104.12.226</connAddr>
        <codecList>
          <codec>8 PCMA/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 39 Connect Ingress Record for Simultaneous Ringing, cont'd

```
<supplementaryService>  
  <servType>SimRing</servType>  
<attemptList>sip:8080@lab2.org:5070;maddr=47.104.12.148+sip:8080@47.102.117  
.196:5060;transport=udp</attemptList>  
  <connParty>sip:8080@lab2.org:5070;maddr=47.104.12.148</connParty>  
</supplementaryService>  
</ipdr:UE>  
</ipdr:IPDR>
```


Figure 40 Connect Ingress Record for Multiple Media (Audio and Video)

```

<ipdr:IPDR seqNum="229" time="2003-03-13T12:10:47Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>normal@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>592266776@lab2.org</uID>
    <corrID>592266776@lab2.org</corrID>
    <recTime>2003-03-13T12:10:32.98Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-13T12:10:26.6Z</startTime>
    <ansTime>2003-03-13T12:10:32.98Z</ansTime>
    <origDest>norma2@lab2.org</origDest>
    <oUA>IMS1.1 Networks FP1 IP Nortel RAIDer/1.1.64</oUA>
    <destinationPhoneNumber>norma2@lab2.org</destinationPhoneNumber>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>nortelnetworks</sessionName>
      <phoneNo>p+1-972-684-1000</phoneNo>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <sdpPort>57348</sdpPort>
        <connAddr>47.104.12.226</connAddr>
        <codecList>
          <codec>18 G729/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 41 Connect Ingress Record for Multiple Media (Audio and Video), cont'd

```
<media>
  <mediaName>video</mediaName>
  <sdpProtocol>RTP/AVP</sdpProtocol>
  <sdpPort>42326</sdpPort>
  <connAddr>47.104.12.226</connAddr>
  <codecList>
    <codec>96 X-NNVC/10</codec>
  </codecList>
</media>
</supplementaryService>
<supplementaryService>
  <servType>SeqRing</servType>
  <attemptList>sip:norma2@47.104.18.108:5060;trans-
port=udp</attemptList>
  <connParty>sip:norma2@47.104.18.108:5060;transport=udp</connParty>
</supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 42 Connect Ingress Record for Authentication

```

<ipdr:IPDR seqNum="34" time="2003-03-13T08:03:11Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>sip03001@auto3app2.com</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>24036714sip09@automation_com</uID>
    <corrID>24036714sip09@automation_com</corrID>
    <recTime>2003-03-13T08:03:15.89Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-13T08:03:11.66Z</startTime>
    <ansTime>2003-03-13T08:03:15.90Z</ansTime>
    <origDest>sip03002@auto3app2.com</origDest>
    <destinationPhoneNumber>sip03002@auto3app2.com</destinationPhoneNum-
ber>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>Nortel Networks</sessionName>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <sdpPort>58784</sdpPort>
        <connAddr>47.104.12.226</connAddr>
        <codecList>
          <codec>0 PCMU/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 43 Connect Ingress Record for Authentication, cont'd

```
<supplementaryService>
  <servType>Authentication</servType>
  <succStatus>>true</succStatus>
</supplementaryService>
<supplementaryService>
  <servType>SeqRing</servType>
  <attemptList>sip:sip03002@auto3app2.com;trans-
port=TCP;maddr=47.104.28.142:16827</attemptList>
  <connParty>sip:sip03002@auto3app2.com;trans-
port=TCP;maddr=47.104.28.142:16827</connParty>
</supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 44 Connect Ingress Record for Redirection

```

<ipdr:IPDR seqNum="138" time="2003-03-13T11:50:37Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>normal@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>529944210@lab2.org</uID>
    <corrID>529944210@lab2.org</corrID>
    <recTime>2003-03-13T11:50:22.12Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-13T11:50:10.40Z</startTime>
    <ansTime>2003-03-13T11:50:22.12Z</ansTime>
    <origDest>norma2@lab2.org</origDest>
    <oUA>IMS1.1 Networks FP1 IP Nortel RAIDer/1.1.64</oUA>
    <destinationPhoneNumber>norma2@lab2.org</destinationPhoneNumber>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>nortelnetworks</sessionName>
      <phoneNo>p+=1-972-684-1000</phoneNo>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <sdpPort>44318</sdpPort>
        <connAddr>47.104.12.226</connAddr>
        <codecList>
          <codec>18 G729/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 45 Connect Ingress Record for Redirection, cont'd

```
<supplementaryService>
  <servType>Redirection</servType>
  <fromAddr>norma2@47.102.117.48:5065</fromAddr>
  <toAddr>norma3@lab2.org</toAddr>
  <connParty>sip:norma3@47.102.117.48:5064;transport=udp</connParty>
</supplementaryService>
<supplementaryService>
  <servType>SeqRing</servType>
  <attemptList>sip:norma2@47.102.117.48:5065;trans-
port=udp</attemptList>
  <connParty>sip:norma3@47.102.117.48:5064;transport=udp</connParty>
</supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 46 Connect Ingress Record for Collaboration

```
<ipdr:IPDR seqNum="175" time="2003-03-13T11:57:10Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>normal@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>69770575@47.104.18.93</uID>
    <corrID>69770575@47.104.18.93</corrID>
    <recTime>2003-03-13T11:56:55.5Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-13T11:56:55.77Z</startTime>
    <ansTime>2003-03-13T11:56:55.95Z</ansTime>
    <origDest>norma2@lab2.org</origDest>
    <oUA>IMS1.1 Networks FP1 IP Nortel RAIDer/1.1.64</oUA>
    <destinationPhoneNumber>norma2@lab2.org</destinationPhoneNumber>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>Collaboration</sessionName>
      <media>
        <mediaName>application</mediaName>
        <sdpProtocol>udp</sdpProtocol>
        <sdpPort>45698</sdpPort>
        <connAddr>47.104.12.226</connAddr>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 47 Connect Ingress Record for Collaboration, cont'd

```
<supplementaryService>
  <servType>SeqRing</servType>
  <attemptList>sip:norma2@47.102.117.48:5065;trans-
port=udp</attemptList>
  <connParty>sip:norma2@47.102.117.48:5065;transport=udp</connParty>
</supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```


Figure 48 Connect Egress Record

```
<ipdr:IPDR seqNum="21" time="2003-03-12T15:59:00Z">
  <ipdr:SS service="ConnectEgress">
    <ipdr:SC xs:type="SC-VoIP-Type"/>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>4769435c_f3e43e0bdc@test2_app1</uID>
    <corrID>532069808@lab2.org</corrID>
    <recTime>2003-03-12T15:58:46.79Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-03-12T15:58:44.62Z</startTime>
    <ansTime>2003-03-12T15:58:46.79Z</ansTime>
    <aband>>false</aband>
    <ansInd>>true</ansInd>
    <outpulsedDigits>8081@lab2.org:5070</outpulsedDigits>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 49 Long Call Ingress Record

```

<ipdr:IPDR seqNum="212" time="2003-01-15T12:14:31Z">
  <ipdr:SS service="LongCallIngress">
    <ipdr:SC xs:type="SC-VoIP-Type"/>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>appsvr</appSrvID>
      <appSrvVer>ims_1.1_build271</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>7d126f6f_f2c305a356@zpvcs006</uID>
    <corrID>52d519ac_f2c305a1cf@zpvcs006</corrID>
    <recTime>2003-01-15T12:09:30.42Z</recTime>
    <endTime>2003-01-15T12:09:30.42Z</endTime>
    <failRsn>408</failRsn>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 50 Long Call Egress Record

```

<ipdr:IPDR seqNum="177" time="2003-01-15T11:48:29Z">
  <ipdr:SS service="LongCallEgress">
    <ipdr:SC xs:type="SC-VoIP-Type"/>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>appsvr</appSrvID>
      <appSrvVer>ims_1.1_build271</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>1774322887@nortelnetworks.com</uID>
    <corrID>1774322887@nortelnetworks.com</corrID>
    <recTime>2003-01-15T11:37:05.46Z</recTime>
    <endTime>2003-01-15T11:37:05.45Z</endTime>
    <failRsn>408</failRsn>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 51 SDP Record for Call Hold

```
<ipdr:IPDR seqNum="61" time="2003-03-13T09:51:18Z">
  <ipdr:SS service="SDP">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>8080@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>1770168785@lab2.org</uID>
    <corrID>1770168785@lab2.org</corrID>
    <recTime>2003-03-13T09:51:03.69Z</recTime>
    <sessionName>nortelnetworks</sessionName>
    <media>
      <mediaName>audio</mediaName>
      <sdpProtocol>RTP/AVP</sdpProtocol>
      <sdpPort>52170</sdpPort>
      <connAddr>0.0.0.0</connAddr>
      <codecList>
        <codec>18 G729/8000</codec>
      </codecList>
    </media>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 52 SDP Record for Call Retrieve

```
<ipdr:IPDR seqNum="62" time="2003-03-13T09:51:22Z">
  <ipdr:SS service="SDP">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>8080@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>1770168785@lab2.org</uID>
    <corrID>1770168785@lab2.org</corrID>
    <recTime>2003-03-13T09:51:07.45Z</recTime>
    <sessionName>nortelnetworks</sessionName>
    <media>
      <mediaName>audio</mediaName>
      <sdpProtocol>RTP/AVP</sdpProtocol>
      <sdpPort>52170</sdpPort>
      <connAddr>47.104.12.226</connAddr>
      <codecList>
        <codec>18 G729/8000</codec>
      </codecList>
    </media>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 53 SDP Record for Web Push

```
<ipdr:IPDR seqNum="103" time="2003-03-13T10:19:39Z">
  <ipdr:SS service="SDP">
    <ipdr:SC xs:type="SC-VoIP-Type">
      <subscriberID>5089@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>6e5dba21_f3e82d1a7b@test2_app1</uID>
    <corrID>112874470@47.104.12.148</corrID>
    <recTime>2003-03-13T10:19:24.75Z</recTime>
    <phoneNo>WebPush</phoneNo>
    <webURI>w=http://www.yahoo.com</webURI>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 54 REFER Record

```
<ipdr:IPDR seqNum="74" time="2003-03-13T09:59:37Z">
  <ipdr:SS service="REFER">
    <ipdr:SC xs:type="SC-VoIP-Type"/>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>61f7bd20_f3e81bbefe@test2_ipcmweb</uID>
    <corrID>61f7bd20_f3e81bbefe@test2_ipcmweb</corrID>
    <recTime>2003-03-13T09:59:22.23Z</recTime>
    <notifyArrival>2003-03-13T09:59:22.23Z</notifyArrival>
    <referBy>sip:5089@lab2.org ; Correla-
tionID=61f7bd20_f3e81bbefe@test2_ipcmweb</referBy>
    <referTo>sip:8081@lab2.org</referTo>
    <referArrival>2003-03-13T09:59:16.37Z</referArrival>
    <referStatus>2</referStatus>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 55 Disconnect Ingress Record

```
<ipdr:IPDR seqNum="23" time="2003-03-12T15:59:05Z">
  <ipdr:SS service="DisconnectIngress">
    <ipdr:SC xs:type="SC-VoIP-Type"/>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>532069808@lab2.org</uID>
    <corrID>532069808@lab2.org</corrID>
    <recTime>2003-03-12T15:58:51.29Z</recTime>
    <endTime>2003-03-12T15:58:51.29Z</endTime>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 56 Disconnect Egress Record

```
<ipdr:IPDR seqNum="24" time="2003-03-12T15:59:05Z">
  <ipdr:SS service="DisconnectEgress">
    <ipdr:SC xs:type="SC-VoIP-Type"/>
    <ipdr:SE xs:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_1.1.5_build332</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xs:type="UE-VoIP-Type">
    <uID>4769435c_f3e43e0bdc@test2_app1</uID>
    <corrID>532069808@lab2.org</corrID>
    <recTime>2003-03-12T15:58:51.30Z</recTime>
    <endTime>2003-03-12T15:58:51.30Z</endTime>
  </ipdr:UE>
</ipdr:IPDR>
```




Performance management

Accounting performance

Accounting performance is monitored through the System Management Console GUI by viewing Operational Measurements (OMs) for the CAM and LAM. Refer to the *MCP System Management Console Basics* for information on OMs and viewing OMs.



Security and Administration

How this chapter is organized

This chapter is organized as follows:

- “Security strategy overview” on page 107
 - “User administration” on page 107

Security strategy overview

The Accounting Module is located on the private managed network, which is located behind a firewall. The Management Module manages the security functions for the Accounting Module. For additional information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics*.

User administration

Basic administrative tasks not defined in the other sections of this document, are detailed in the *MCP System Management Console Basics*.

Succession Multimedia Communications Portfolio

MCP Accounting Module

Basics

Copyright © 2003 Nortel Networks,
All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the MCP Accounting Module without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, UNISim, MCP, Nortel, Northern Telecom, and NT, are trademarks of Nortel Networks.

Publication number: NN10037-111
Product release: MCP 1.1 FP1 Standard
Document release: Standard MCP 1.1 FP1 (02.02)
Date: April 2003
Printed in the United States of America.

